COMPAQ

Netelligent Management Software

User Guide

NOTICE

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication contains information protected by copyright. No part of this publication may be photocopied or reproduced in any form without prior written consent from Compaq Computer Corporation.

The software described in this guide is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement.

Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

©1997 Compaq Computer Corporation.
All rights reserved. Printed in the U.S.A.

Compaq, Compaq Insight Manager, SmartStart, and ProLiant are registered United States Patent and Trademark Office.

Netelligent and ProSignia are trademarks and/or service marks of Compaq Computer Corporation.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Compaq Netelligent Management Software User Guide

Fourth Edition (June 1997)
Part Number 475A/0697

Contents

Chapter 1
Introduction

Installation Requirements 1-2
Installing Netelligent Management Software 1-3
Windows 95 1-3
Windows NT 1-4
Using the Online Documentation 1-4

Chapter 2
Guided Tour

Starting Netelligent Management Software 2-1
Using the Main Window Controls 2-2
Menu Bar 2-2
Button Bar 2-2
Network Devices Window 2-3
Network Workspace Window 2-7
Network Holding Area 2-7
Map Right-Click Menu 2-7
Using Online Help 2-8
Working with Network Maps 2-9
Creating a Single Network Map 2-9
Creating Sub-Maps 2-10
Connecting Devices Across Maps 2-11
Changing Map Properties 2-12
Printing a Map 2-13
Importing a Map File 2-14
Using the Draw Mode 2-14
Using the Move Mode 2-14
Using the Site Right-Click Menu 2-15

Working With Devices 2-16
Using the Device Right-Click Menu 2-16
Viewing General Device Properties 2-16
Viewing Device Supported MIBs 2-18
Viewing Device Mappable Ports 2-18
Viewing SNMP Information for a Device 2-18
Viewing Device Health Polling 2-19
Using IP Discovery 2-19
Finding a Network Entity 2-20
Pinging a Device 2-22
How to Telnet to a Device 2-22
Viewing Mapped Devices 2-23
Displaying a Netelligent Device 2-23
Deleting a Device 2-24
Working With SNMP Statistics 2-25
Device System Information 2-25
Device Interface List 2-26
Interface Statistics 2-27
Viewing SNMP Traffic Statistics 2-28
Viewing Repeater Port Statistics 2-29
Viewing Repeater Errors 2-30
Creating a Static Route 2-33
Protocol Information 2-33
Working With Graphs 2-42
Starting the Graphing Function 2-42
Setting Graph Thresholds 2-42
Hiding a Graph 2-44
Printing a Graph 2-44
Exporting Graph Data to a File 2-45
Viewing Running Graphs 2-45
Setting Graph Polling Options 2-46
Selecting Graph Styles 2-47
Setting Graph Colors 2-47

Using the Compaq Common MIB 2-49
Compaq Devices Information 2-49
Supported MIB Modules 2-50
Setting SNMP and IP Access 2-50
Configuring an IP Address 2-51
Configuring an IPX Address 2-52
Configuring a Serial Port 2-52
Viewing Component Version Information 2-53
Setting IP and IPX Trap Destinations 2-53
Configuring BootP 2-54
Configuring TFTP 2-55
Using Netelligent Management Software Utilities 2-56
Configuring a BootP Server 2-56
Enabling BootP 2-57
Setting Up Health Polling 2-57
Enabling Health Polling 2-58
Changing the Color for Device Status 2-58
Pinging All IP Addresses 2-59
Determining a Device Type 2-59
Changing a Mapped Device Type 2-60
Showing State Colors 2-60
Enabling TFTP 2-60
Making TFTP Transfers 2-60
Starting the MIB Browser 2-60
Compacting the ODBC Database 2-61
Using the Event Log Viewer 2-63
Setting Event Log Viewer Filters 2-64
Exporting Event Log Entries 2-68
Viewing Event Log Entry Details 2-71
Deleting Events 2-71
Clearing Alarms 2-71
Resynchronizing Alarms to the Database 2-72
Setting the Maximum Number of Event Log Entries 2-72

Chapter 3
Managing Netelligent Hubs and Switches

Context-Sensitive Help 3-1
Operation Fundamentals 3-2
Displaying a Netelligent Product Graphic 3-2
Using the File Menu 3-3
Using the Help Menu 3-3
Using the Button Bar 3-4
Refreshing the Display 3-4
Setting the Auto Poll Rate 3-4
Enabling Auto Polling 3-5
Viewing the Stack Configuration 3-5

Chapter 4
Using the MIB Browser

Online Help 4-2
Context-Sensitive Help 4-2
MIB Browser Description 4-2
Main Window 4-3
Hands-On Examples of the MIB Structure 4-9
Using MIB Browser Tools and Menus 4-14
Selecting a MIB to Manage the Agent 4-21
Adding and Removing Currently Compiled MIBs 4-22
Parsing a MIB 4-22

Chapter 5
Using MIB Browser Reports

Creating Reports 5-1
Starting an Existing Report 5-3
Defining Custom Reports 5-5
Designating Default Reports 5-11
Deleting a Report 5-13
Working With Reports 5-14

Viewing a Report as a Table, Graph, or Dial 5-14
Editing Report Thresholds 5-20
Exporting Report Data 5-24
Working With Dial and Graph Reports 5-30
Working With Table Reports 5-47
Selecting a Font 5-56
Printing a Report 5-57
Closing a Report 5-57

Chapter 1
Introduction

Compaq Netelligent Management Software is a 32-bit, SNMP management application for Windows 95 and Windows NT (v3.5.1 or later). The software uses an intuitive, easy-to-use design to deliver high-performance network management of Compaq Netelligent hubs, switches, and routers. Engineered for the latest Netelligent network technology, Netelligent Management Software supports the full line of manageable Compaq Netelligent products. It provides the following important features:

- Drag-and-drop graphical user interface for fast network map configuration
- Hierarchic network topology views to help you organize and manage large networks on your management console
- Full-featured event log database with filtering and exporting capabilities
- New innovative real-time performance graphing capability with threshold facilities
- Step-by-step Netelligent 8500 configuration wizard
- Integrated BootP and TFTP facilities
- New device type verification feature can validate an icon on the map against the physical device
- Automated Internet Protocol device discovery greatly speeds network management setup
- MIB compiler and browser enhancements make easy work of handling MIB data
- Product Management Module architecture for easy software updates as you add new Netelligent products to your network

Installation Requirements

Netelligent Management Software requires the following hardware and software for a correct installation:

- Intel 486 or later processor
- CD-ROM drive
- At least 40 megabytes of available fixed disk drive space
- At least 16 megabytes of RAM (24 MB RAM recommended)
- Windows 95 or Windows NT 3.51 (or greater) running on the management worsktation

Installing Netelligent Management Software

To install Netelligent Management Software, use the procedure below that corresponds to your management workstation's operating system. During the software installation, you have the option of installing Compaq Netelligent Management Software online user documentation and the Adobe Acrobat Reader, which lets you view or print the documentation.

Windows 95

Follow these steps to install Netelligent Management Software on a workstation that is running Windows 95.

1. Insert the Compaq Netelligent Management Software CD into the CD-ROM drive. The installation program starts automatically. Follow the instructions on the screen to complete installation.

   NOTE: If the installation program does not start automatically, follow Steps 2 through 4.

2. Click on the *Start* button, then select *Run*.
3. Type D:\SETUP.EXE (where D is the CD-ROM drive letter) and select *Enter*.
4. The resulting screens guide you through the installation procedure. Follow the instructions on the screens to complete installation.

The installation program automatically creates a Netelligent Management Software icon in the appropriate Windows screen.

Windows NT

Follow these steps to install Netelligent Management Software on a workstation that is running Windows NT v3.5.1 or greater.

1. Insert the Compaq Netelligent Management Software CD into the CD-ROM Drive. For Windows NT v4.0, the installation program starts automatically. Follow the instructions on the screen to complete installation.

   NOTE: If the installation program does not start automatically, follow Steps 2 through 4.

2. From File Manager, select *File*, then select *Run*.
3. Enter D:\SETUP.EXE (where D is your CD-ROM drive).
4. Follow the instructions on the screen.

The installation program automatically creates a Netelligent Management Software icon in the appropriate Windows screen.

Using the Online Documentation

Netelligent Management Software user documentation is included online as an Adobe Acrobat (PDF) file on the Compaq Netelligent Management Software CD. If you install the Adobe Acrobat Reader, you can view or print the documentation.

To view the user guide, start the Adobe Acrobat Reader and open the file USRGUIDE.PDF from the USRGUIDE sub-directory in the main directory where you installed Netelligent Management Software (C:\NETMGR, for example). Or, open the file from the D:\USRGUIDE directory (where “D” is the letter of the CD-ROM drive).

You can order a bound hard copy of the main user guide (Part No. 220A/0197) from your Compaq Authorized Reseller.

Chapter 2
Guided Tour

Starting Netelligent Management Software

You can run Netelligent Management Software by itself or from within Compaq Insight Manager.

To run Netelligent Management Software on a standalone management workstation where Compaq Insight Manager was not installed, select the Netelligent Management Software option from the Windows Start/Programs menu.

To run Netelligent Management Software from within Compaq Insight Manager, select the Netelligent Management Software program icon from the button bar in Server List window of Compaq Insight Manager.

NOTE: The icon appears on the Compaq Insight Manager button bar only if Compaq Insight Manager was installed before you installed Netelligent Management Software.

Using the Main Window Controls

When you start Netelligent Management Software, the main window appears. This window is made up of four disctinct sections:

- Menu Bar
- Button Bar
- Network Devices window
- At least one Network Workspace (map) window

Menu Bar

The Netelligent Management Software menu bar contains menus that list the main commands and other functions. Click on a menu name to view a list of menu options.

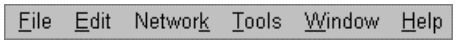


Figure 2- 1. Menu Bar

The Edit menu appears only when you highlight a device icon on a network map. This menu includes several device-related functions. A graphing menu is also available when you display interfaces statistics screens for various Netelligent products. The graphing menu lets you monitor different types of statistical information in real time.

Button Bar

The button bar contains shortcuts to commands used most often. Click on a button to display a window for the associated command. The button bar commands are also available as menu options. For a brief description of a button's function, position the mouse pointer over the button.

Figure 2- 2. Button Bar

Network Devices Window

The Network Devices Window shows a group of icons you can use during your network configuration and management. These icons are divided into four categories: Sites, Hosts, Devices, and LAN/WAN media. You can display as many of these categories as you like. To view icons for a particular category, click on the checkbox next to the category name at the top of the window.

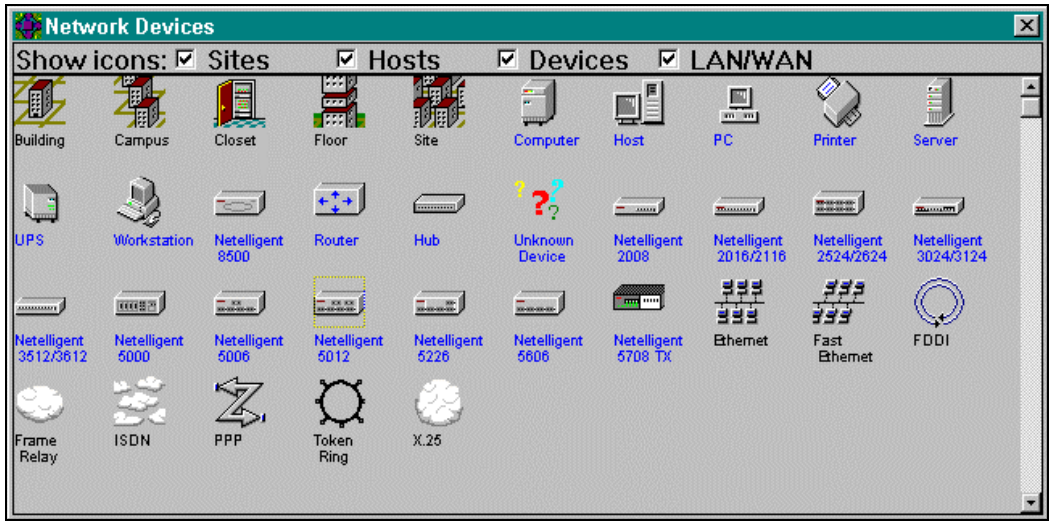


Figure 2- 3. Network Devices Window

Below are the descriptions of each icon contained in the Netelligent Management Software Network Devices window:

Site Icons

The site icons represent the various levels of a network—from the aggregate network installation to an individual wiring closet.

Site represents an entire network installation.

Campus represents a specific campus within a site.

Building represents a specific building on a campus.

Floor represents a specific floor in a building.

Closet represents a specific location for devices and their associated wiring.

Host Icons

The host icons represent various hosts common to networks, including shared devices such as printers and servers, as well as client workstations.

Computer

Host

PC

Printer

Server

UPS

Workstation

Device Icons

The device icons represent the actual network communication devices in your network, including hubs, switches, and routers. As you add PMMs (program management modules) for new Netelligent devices, the corresponding device icons appear in the window.

Netelligent 8500 Router

Netelligent 2008 Hub

Netelligent 2016/2116 Hub

Netelligent 2524/2624 Hub

Netelligent 3024/3124 Hub

Netelligent 3512/3612 Hub

Netelligent 5000 Switch

Netelligent 5006 Switch

Netelligent 5012 Switch

Netelligent 5606 Switch

Netelligent 5708 Switch

Generic Router

Generic Hub

Unknown Device

LAN/WAN Icons

The LAN/WAN icons represent various networking topologies and protocols supported by Netelligent Management Software.

Ethernet Connection (LAN)

Fast Ethernet Connection (LAN)

Token Ring (LAN)

FDDI Connection (WAN)

Frame Relay Connection (WAN)

ISDN Connection (WAN)

X.25 Connection (WAN)

PPP (Point to Point Protocol) Connection

Network Workspace Window

The Network Workspace window is the area where you create network maps and perform network management for specific network entities. When you first start Netelligent Management Software, this area (named Main) is blank. For information about creating a network map, see "Working with Network Maps."

Network Holding Area

The Network Holding Area displays devices that meet the following criteria when you start the software:

- Devices that request BootP service, including IP addresses and configuration files (if the BootP server is enabled)
- Devices that have been discovered via IP discovery
- Unmapped devices that have sent traps

You can also display this window by selecting *Window/Network Holding Area* from the menu bar. To clear the holding area, select *Clear Holding Area* from the Network menu or exit the software.

Map Right-Click Menu

You can access many of the same map-related functions available from the Edit menu by clicking the right mouse button on an area of the map that is not an icon (when the pointer is a hand icon). The following menu appears.

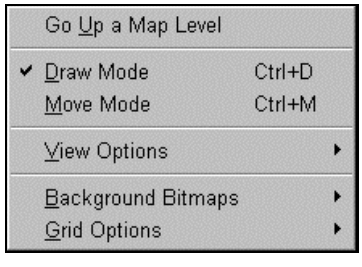


Figure 2- 4. Map Right-Click Menu

In addition to the Edit menu functions, this menu also provides a *Go Up a Map Level* option which lets you display a higher level map if you display the menu from a sub-map.

Using Online Help

While you work with Netelligent Management Software, you can get online help in the following ways:

- Select the **F1** key to display the main online help window.
- Select an option (*Contents*, *Module Information*, or *About*) from the *Help* menu on the menu bar.

Contents - Select *Help/Contents* to view the list of online help topics.

Module Information - Select *Help/Module Information* to display a Netelligent Management Software version summary for the selected device.

About - Select *Help/About* to view information about the software.

Click on the Help button (question mark) to display the main online help window.

View the status bar at the very bottom of the window for immediate information about the current function.

Working with Network Maps

Netelligent Management Software uses *network maps* to represent the actual physical configuration of your network. You can create a single map for a basic network, or you can create multiple hierarchical *sub-maps* that represent several levels of a much larger network.

Creating a Single Network Map

The software's drag-and-drop interface lets you create a network map by connecting icons that represent network entities (for example, devices, protocols, or sites) on the map. When you connect two icons, the software instantly prompts you for the required information or alerts you of any invalid connections. To create a map, follow these steps:

1. From the Network Devices window, click on an icon and hold down the left mouse button.
2. Drag the icon to the network workspace and release the mouse button. A description box appears.
3. Enter the description for the entity and click on *OK*.
4. Return to the Network Devices window and select another entity you would like to add to the network map. Then repeat Steps 1-3 to move the next icon to the workspace.
5. To connect the two icons, select the draw mode by clicking on the Draw button. Then place the pointer over one of the icons. The pointer changes to a pencil.
6. Click and hold down the left mouse button as you "draw" a line to the other icon. When the cursor is over the other icon, release the mouse button. If the connection is valid, the Connect Network Entities dialog box appears. This box shows the description of the two devices and the available connection points.

You can now enter specific connection information, such as the connection port and IP address and net mask of the device.

If the connection is not valid, an error message either states that the two entities cannot be linked or that they cannot be physically connected and gives you the option of viewing connection information.

Creating Sub-Maps

The following illustration shows an interstate network configuration with sites in California, Texas, and New York. The displayed *sub-maps* show each subsequent hierarchical level from state (Texas) to city (Houston) to campus (Campus #1) to floor (Accounting Floor). In this example, the floor level displays the specific devices and media for that network configuration.

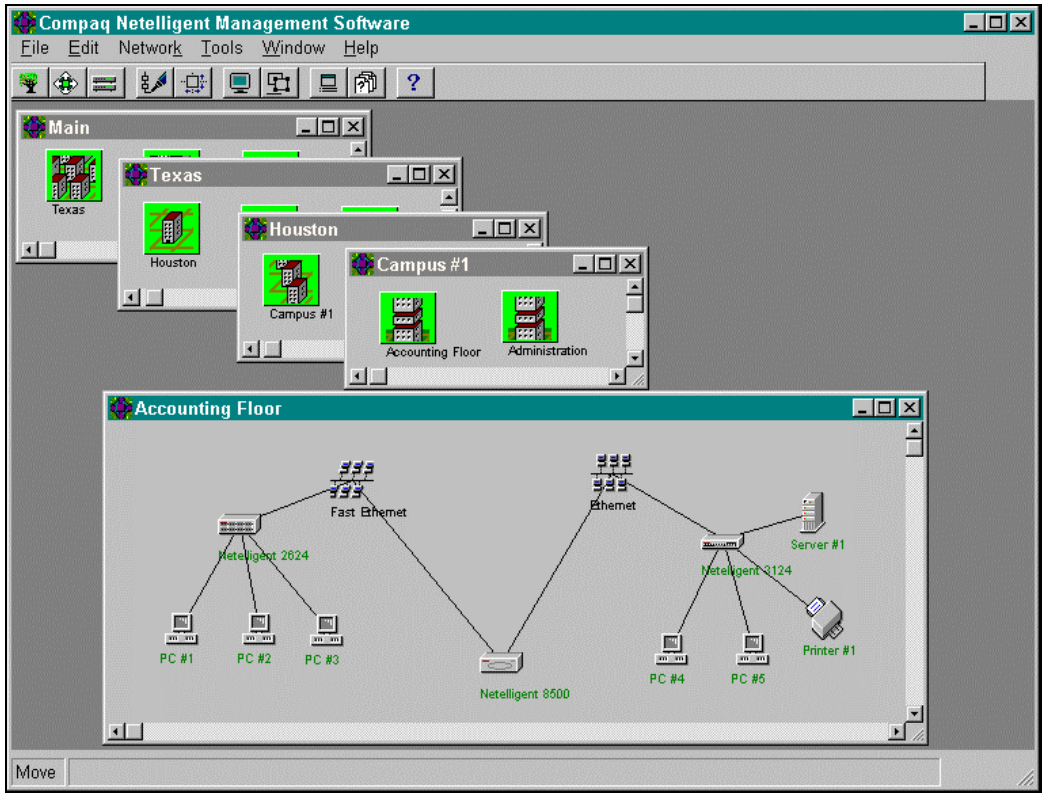


Figure 2- 5. Network Maps and Sub-Maps

To create a sub-map, follow these steps:

1. Drag and drop a site icon (Site, Campus, Building, Floor, or Closet) from the Network Devices window to the main map (or existing sub-map). The following message appears:

   Name the sub-map that you want this site icon to represent in your network.

2. Enter the desired name and click on *OK*. The software places the icon on the map and creates a new sub-map with the same name. You can now build a network on the new sub-map or create more sub-maps as needed.

Connecting Devices Across Maps

You can also connect devices from map to map (window to window). To do so, draw the connection line between icons just as you would within a single map. When you draw a successful connection, the interlink icon (Campus #1 icon in the following illustration) appears on the lower level sub-map along with the name of the higher level map and the name of the device on that map you connected to. On the higher level map, the software automatically draws a line from the connected device to the icon that represents the lower-level sub-map. The following example shows a Netelligent 8500 router on the Campus #1 sub-map connected to a Fast Ethernet LAN on the Accounting Floor sub-map.

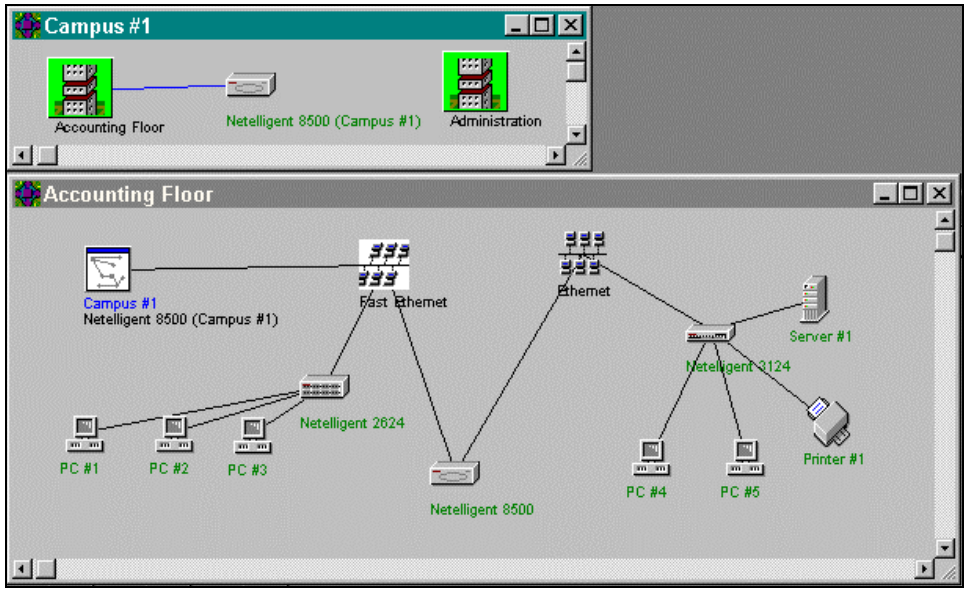


Figure 2- 6. Sub-Map Example

Changing Map Properties

The Map Properties menu lets you determine how objects appear on the currently active map.

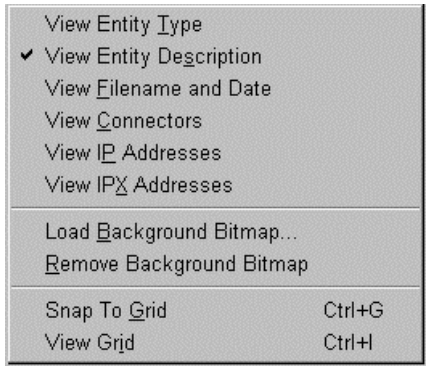


Figure 2- 7. Map Menu

Selecting View Options

The first part of the menu (View options) lets you control the amount of information that appears on the currently active map. Click on the option for the information you want to view.

Loading a Background Bitmap

You can select a unique bitmap image (Windows BMP file) as the background for the currently active map.

To load a background bitmap image, select *Load Background Bitmap*. In the resulting dialog box, select the desired bitmap and click on *Open*.

To remove the background bitmap, select *Remove Background Bitmap*. When the Confirm box appears, click on *Yes* to remove the image.

Using Map Grids

You can arrange network device icons on a map by aligning them with a map grid. This allows a more precise map layout, especially if the map contains many icons. To view the grid, select *View Grid*.

The grid snap function facilitates icon alignment by forcing the icons to conform to the grid lines. To turn on the grid snap function, select *Snap to Grid*. Then, in the move mode, move each individual icon to the desired square. You can also use grid snap function when the grid is not visible

Printing a Map

To print the current map to your default Windows printer, select *File/Print Map*. Then click on *OK* when the confirmation box appears.

Importing a Map File

To import a map file from an earlier version of Netelligent Management Software (1.2 or earlier), select *File/Import a 1.x MAP File*. Then select the desired map file from the dialog box and click on *OK*. The imported map appears as a sub-map of the main window.

Using the Draw Mode

The draw mode lets you connect two objects within the same map or from one map to another. To select the draw mode, click on this option so that a checkmark appears next to the option. Or, click on the Draw Mode button from the button bar. The cursor changes to a pencil.

To connect two objects, click on one of the objects. Then, hold down the left mouse button and draw a line to the other object. If the connection is valid, the Connect Network Entities dialog box appears. If the connection is not valid, an error message appears.

Using the Move Mode

The move mode lets you move individual device icons on a workspace. To select the move mode, click on this option so that a checkmark appears next to the option. Or, click on the Move Mode button from the button bar. The cursor changes to two intersecting, double-ended arrows.

To move an icon, click on the icon. Then, hold down the left mouse button and move the icon where desired.

To move all icons on a map, move the pointer anywhere on the map except on an icon. The pointer displays a “hand” icon. Click and hold down the left mouse button and move the icons where desired.

Using the Site Right-Click Menu

The site right-click menu lets you quickly perform site-related map functions.

Properties – Select to display a general description of the site.

Open Site Map – Select to view the map related to the site or to display the map as the active window.

Delete – Deletes the site icon from the map. If the site map contains icons for network entities, an error message appears stating that the map the icon represents is not empty. If you still want to delete the map, first delete the objects from the map. Then try the delete function again.

NOTE: You can also selectively and quickly delete icons using the Find Network Entity dialog box. See "Finding a Network Entity."

Working With Devices

This section discusses functions that apply to specific networking devices.

Using the Device Right-Click Menu

The device right-click menu provides similar functionality as the Edit menu on the main menu bar. To view the right-click menu, click the right mouse button on the device icon. The menu provides the following options:

Properties — Displays the Device Properties dialog box.

Delete Device — Deletes the device from the network map. See "Deleting a Device."

Configuration — Displays the configuration sub-menu for configuring a Netelligent 8500 router. See "Starting the Guided Configuration for a Netelligent 8500 Router."

SNMP Statistics — Displays the SNMP sub-menu which provides access to all SNMP- and MIB-related functions. See "SNMP Statistics."

Utilities — Displays the Utilities sub-menu for access to communication and status utilities.

View Log File — Opens an Event Log Viewer which displays entries for the selected device.

Image Firmware Options — Displays the Netelligent 8500 Software Management Options dialog box (if the device supports this option).

Viewing General Device Properties

The General tab of the Device Properties dialog box displays basic information about a device and its connections. It also lets you delete or move circuits or connections to the device. To display the Device Properties box, select *Edit/Properties* or select *Properties* from the device right-click menu.

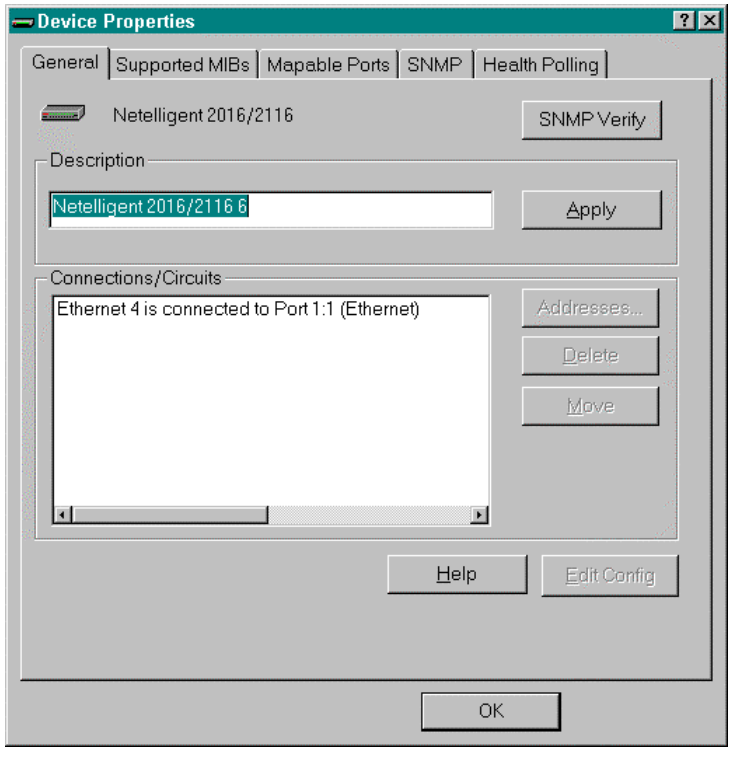


Figure 2- 8. Device Properties Dialog Box

Description — A freeform description of the device

SNMP Verify — Queries a device's sysObjectID and sysServices information through SNMP to determine what type of device it is. See "Determining a Device Type."

Connections/Circuits — Lists the device, port it is connected to, and other device(s) connected to it.

Addresses — Select this option to view or edit hardware layer addresses.

Delete — Deletes the selected circuit or connection.

Move — Changes the connection of the device to other available ports.

NOTE: You must select a connection/circuit to enable the Addresses, Delete , and Move buttons.

Viewing Device Supported MIBs

The Supported MIBs tab of the Device Properties dialog box lets you add and/or remove MIBs that the selected device supports.

Viewing Device Mappable Ports

The Mappable Ports tab of the Device Properties dialog box shows the available ports on the device that can be mapped. The lower area displays the available media for the selected port.

INI File — The INI file for the selected device. This file stores configuration information for the device if the guided configuration was used.

Configuration — The device configuration, if applicable.

Viewing SNMP Information for a Device

The SNMP tab of the Device Properties dialog box lets you change SNMP read and write community strings as well as the time out and retries used for SNMP communications. You can also select the address used for health polling and other SNMP communications from a list of all available IP addresses on device with multiple addresses.

Address — The address used for SNMP communication

Read Community — The SNMP read community string that lets you read SNMP information

Write Community — The SNMP write community string that lets you read or write SNMP information

Time Out — Amount of time the device waits before a retry

Retries — Number of retries

Viewing Device Health Polling

The Health Polling tab of the Device Properties dialog box lets you configure health polling for any device. If it is enabled, the software sends an SNMP request to the device based on the polling Interval selected. If a device is polled and responds, the background of the device icon turns green. If a device is polled and fails to respond, the background of the device icon turns red. You can change the colors that the device icons display. See "Changing the Color for Device Status."

Health Polling — Sends an SNMP request for system up time (either enabled or disabled).

Poll Every — The interval time period (seconds) to send a health poll.

Send Alarm — Informational, Indeterminate, Minor, Major, Critical. If the poll fails, the software logs one of these alarms.

Using IP Discovery

The IP discovery function uses SNMP queries to discover IP nodes. You can start IP discovery from the Network/IP Discovery menu option or from the right-click menu for a particular device, such as an IP router. As the software discovers nodes, it places icons that represent the nodes in the Network Holding area.

You can specify that the software discover all nodes within a certain number of router hops of the starting node or that it discover a list of networks. To enable IP discovery, you must provide the following information:

Starting Gateway — The first IP address the software queries. The node at this IP address must support SNMP and preferably have router functionality. If you use the device right-click menu to access IP discovery, this field will already be filled in.

Read Community — An SNMP community name to be used for all SNMP requests. The default value is "public."

Timeout — The timeout value, in seconds, to be used for all SNMP requests. This value can have considerable impact on the overall discovery process. When the software discovers IP addresses that do not support SNMP, the discovery function times out. A smaller timeout value speeds the discovery process but also limits the number of IP addresses that can be discovered. The default value is 5 seconds.

Retries — The number of times the software retransmits a query after a timeout. This value can have a considerable impact on the overall discovery time. That is, the more retries, the longer the discovery time. The default value is 0.

If you specify maximum repeater hops, you must also provide the following information:

Gateway Mask — The network mask for the starting IP address.

LAN Hops from Gateway — The maximum number of LAN hops from the starting IP address which will be traversed during the discovery process. This field lets you limit the discovery. A value of 0 (default) discovers all nodes on the same network as the starting IP address. However, the software might also discover nodes in adjacent networks, but these are not queried.

Filtering Unmanaged Devices During IP Discovery

To prevent the software from displaying unmanaged devices in the Network Holding area during IP discovery, select *Tools/Preferences* to display the Properties dialog box. In the General tab, click on the checkbox so that a checkmark appears.

Finding a Network Entity

To search for one or more network entities such as a device or topology type, select *Tools/Search*. The resulting dialog box lets you specify the attributes the search function uses to find the entity or entities.

Description — The description of the specific entity you want to locate (for example, Netelligent 5708 Switch). You can designate the description as case-sensitive to allow a more detailed search.

Device State — The operational status of a particular entity (for example, cleared or minor). To search for entities in all states, select "*(All)*."

Location — The physical location of the entity. This could be a location indicated by the name of a sub-map that contains the icon for the entity. To search for entities in all locations, select "*(All)*."

IP Address — The IP address for the node.

IPX Network — The IPX network address for the node.

Device Type — The type of device you are trying to locate. This list is the same as the list of icons that appear in the Network Devices window. To search for all device types, select "*(All)*."

After you enter all the desired search attributes, click on *Go* to start the search. The search results appear in the lower window.

To view the map for a located entity, double-click on the search result.

Clearing Between Searches

The *Clear between searches* checkbox lets you clear all search results before you start another search. To enable this function, click on the checkbox so that a check appears.

To retain results from a previous search, click on the checkbox so that the check disappears. This lets you build on a previous search by making a subsequent search without clearing the results from the previous search. For example, in your first search, you could search for all entities with an address that started with "198.*". In the next search, you could search for all entities with an address that started with "190.*". The Search Results area displays the results from both searches.

Deleting Entities

To delete an entity from the Search Results window (and from the network map), highlight the desired entry and click on *Delete*. To delete all entities from the Search Results window, click on Delete All. A confirmation box prompts you to confirm or cancel the delete functions.

Using Wildcards

If you are not sure about a description or an IP or IPX address for a particular node, you can use a wildcard (*) character at any point in the search field. For example, in the description field, you might enter “Main*”, or, in the IP address field, you might enter “198.100.*”.

Pinging a Device

Pinging a device lets you know if the device is “alive” on the network, that is, if it has a valid IP address that allows it to communicate with other devices.

To ping a device, click on the device icon. Then select *Ping device* from the Edit menu. The software launches the Windows 95 MS-DOS application and pings the device. The results of the ping appear after the software determines the status of the device.

How to Telnet to a Device

Telnet lets you perform certain management functions such as remote firmware downloads.

To initiate a Telnet session with a device, click on the device icon. Then select *Telnet to this device* from the Edit menu. The software launches the Windows 95 Telnet application which begins communication with the device. When communication is established, proceed with the desired Telnet operations.

Viewing Mapped Devices

To view a list of all devices mapped in a specific network, select *Tools/Mapped Device List* to display the Device Selection window. This window includes all devices contained in the network maps. If other PCs or portables were used to configure devices on the network, the information from those configuration sessions is not displayed. In those cases, you can manually add devices to the network maps.

The window shows the following information about each device:

Device — The description of the device given to it when it was configured

Address — The IP address assigned to the device when it was configured

Device Type — A description of the device based on its function and manufacturer (for example, Netelligent repeater or Netelligent switch)

Config File — The name and location of a configuration file associated with the device. This file could have been generated by Netelligent Management Software or previously downloaded from the device.

Device State — This indicates whether or not the device is responding.

Community — The SNMP read community string for this device

Health Poll — The interval, in seconds, that the device is polled by the management workstation

Location — The physical location of the device

Displaying a Netelligent Device

Netelligent Management Software lets you display accurate graphical representations of Netelligent products, complete with the current LED status and any installed components. In addition to providing physical views of Netelligent products, the software lets you view various types of information, such as configuration settings, port statistics, and system information, by clicking the mouse pointer on control buttons or *hotspots*, which are located on the product graphics.

To display the graphic for the Netelligent switch or repeater you want to manage, double-click on the product icon on a network map.

In order for the product graphic to appear, it must have a valid IP address.

For more information about managing a specific Netelligent device, select the Help menu from the device graphic.

Deleting a Device

To delete a device from a map, do any of the following:

- Click on the device icon. Then press <Del> or select *Delete Device* from the Edit menu.
- Click the right mouse button on the device icon. Then press <Del> or select *Delete Device* from the right-click menu.

When the Confirm box appears, click on *Yes* to delete the device.

You can also delete devices using the search function. See “Deleting Entities” under “Finding a Network Entity.”

Working With SNMP Statistics

This section discusses the SNMP functions and statistics you can monitor and manipulate via Netelligent Management Software. You can display the following dialog boxes by selecting the *SNMP Statistics* option from the Edit menu or from the device right-click menu. You can also display certain dialog boxes (such as Device System Information) from the button bar.

Device System Information

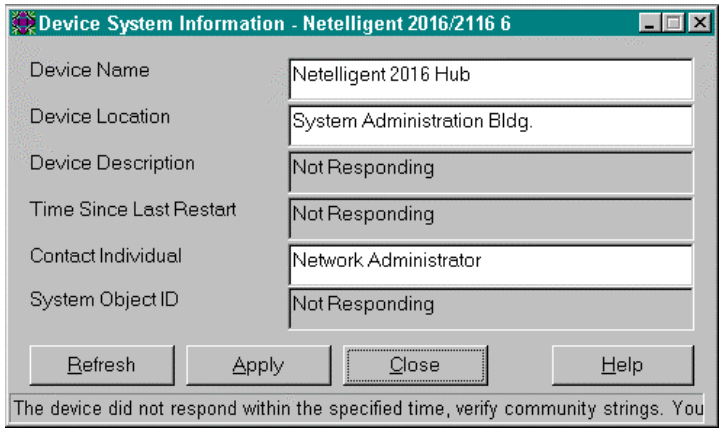


Figure 2- 9. Device System Information Dialog Box

This dialog displays important information that may be useful in managing network devices. The following fields contain this information:

Device Name — The system name of the selected device.

Device Location — The location of the selected device.

Device Description — The type of software running on the selected device.

Time Since Last Restart — The amount of time since the device was restarted or powered on.

Contact Individual — The person's name to contact about this device.

System Object ID — A unique identifier for the SNMP agent running on the device.

Refresh — Updates the values on this dialog.

Save — Allows you to change the Device Name, Device Location, or Contact Individual fields.

Device Interface List

This dialog box displays information for all the interfaces of the current device. To view graphing options for an interface, right-click on the interface entry or select an option from the Graphing menu which appears when you open the dialog box.

Interface Identifier — The unique numerical identifier for the interface.

Interface Type — The type of interface (that is, Ethernet, Frame Relay, FDDI, Serial)

Description — A description of the interface.

Interface Speed — An estimate of the interface's current bandwidth in bits per second. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this field should contain the nominal bandwidth.

Hardware Address — The physical or MAC address of the interface. For interfaces that do not have such an address (for example, a serial line), this field is blank.

Operational Status — The operational status of the interface, either operational or not operational.

Administrative State — The desired administrative status of the interface, either running or down. To change the value of this field, select Down, Operational, or Testing and click on Apply to update the device status. **Caution**: Changing this setting to Down can disrupt data to or from the device.

Refresh — Updates the values on this dialog.

Interface Statistics — Displays more detailed information on the selected interface.

Interface Statistics

This dialog box lets you view the following information about the selected interface. You can also right-click on a data field to view graphing options for the selected interface:

Interface ID — The unique numeric character(s) identifier for the interface in use.

Interface Type — The type of interface in use (i.e., Ethernet, Frame Relay, FDDI, Serial)

Input Statistics

Bytes Received — The number of octets received on this interface

Unicast Packets — The number of unicast packets delivered

Multicast Packets — The number of multicast or broadcast packets delivered to a higher-layer protocol

Error Packets — The number of inbound packets containing a formatting error that prevented them from being delivered to a higher layer protocol

Discarded Packets — The number of inbound packets discarded to prevent their being delivered to a higher layer protocol even though no errors were detected. A reason for this could be resource limitations such as inadequate buffer space.

Unknown Protocols — The number of packets received through this interface that were discarded because of being destined for an unknown or unsupported protocol

Output Statistics

Bytes Sent — The number of octets sent on this interface including framing characters

Unicast Packets — The number of packets that higher level protocols requested to be transmitted to a subnetwork unicast address, including those that were discarded or not sent

Multicast Packets — The number of packets that higher level protocols requested to be transmitted to a subnetwork multicast or subnetwork broadcast address, including those that were discarded or not sent

Error Packets — The number of outbound packets discarded due to a formatting error

Discarded Packets — The number of outbound discarded to prevent their being delivered to a higher layer protocol even though no errors were detected. A reason for this could be resource limitations such as inadequate buffer space.

Refresh — Updates the values on this dialog.

Reset Counters — Resets the current values on this dialog to zero.

Options\Polling Setup — Opens the Polling Parameter Setup dialog, where you can specify how you want the parameter dialog to refresh.

Viewing SNMP Traffic Statistics

To view SNMP traffic statistics, select *Edit/SNMP Statistics/Protocols* or select *SNMP Statistics/Protocols* from the device right-click menu to view the Protocols screen. Click on the SNMP button from the Internet Layer section to view the SNMP Statistics window.

Snmp Input Packets — The total number of messages delivered to the SNMP entity from the transport service.

Snmp Output Packets — The total number of SNMP messages that were passed from the SNMP protocol entity to the transport service.

Bad Community Names — The total number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to the entity.

Read Only Errors — The total number valid SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly.

NOTE: It is a protocol error to generate an SNMP PDU that contains the value readOnly in the error-status field. This object is provided as a way to detect incorrect implementations of the SNMP.

Bad Values — The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.

Set Requests — The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity.

Enable Auth Fail Traps — Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information; providing a way to disable all authentication-failure traps.

Viewing Repeater Port Statistics

To view repeater port statistics, select *Edit/SNMP Statistics/Protocols* or select *SNMP Statistics/Protocols* from the device right-click menu to view the Protocols screen. Click on the *Repeater* button from the Data Link Layer section to view the Port Statistics window.

Repeater ID - This object identifies the group that contains the port for which this entry contains information.

Port Number - This object identifies the port within the group for which this entry contains information.

Readable Frames - This object is the number of frames of valid frame length that have been received on this port. This counter is incremented by one for each frame received on this port whose OctetCount is greater than or equal to minFrameSize and less than or equal to maxFrameSize (Ref: IEEE 802.3 Std, 4.4.2.1) and for which the FCSError and CollisionEvent signals are not asserted.

This statistic provides one of the parameters necessary for obtaining the packet error rate. The approximate minimum time for rollover of this counter is 80 hours.

Collisions - This counter is incremented by one for any CarrierEvent signal on any port for which the CollisionEvent signal on this port is also asserted. The approximate minimum time for rollover of this counter is 16 hours.

Readable Octets - This object is the number of octets contained in valid frames that have been received on this port. This counter is incremented by OctetCount for each frame received on this port which has been determined to be a readable frame (that is, including FCS octets but excluding framing bits and dribble bits).

This statistic provides an indicator of the total data transferred. The approximate minimum time for rollover of this counter is 58 minutes.

Viewing Repeater Errors

To view repeater errors, select *Edit/SNMP Statistics/Protocols* or select *SNMP Statistics/Protocols* from the device right-click menu to view the Protocols screen. Click on the *Repeater* button from the Data Link Layer section to view the Port Statistics screen. Then click on the *Errors* button.

Repeater ID - This object identifies the group that contains the port for which this entry contains information.

Port Number - This object identifies the port within the group for which this entry contains information.

FCS Errors - This counter is incremented by one for each frame received on this port with the FCSError signal asserted and the FramingError and CollisionEvent signals deasserted and whose OctetCount is greater than or equal to minFrameSize and less than or equal to maxFrameSize (Ref: 4.4.2.1, IEEE 802.3 Std).

Alignment Errors - This counter is incremented by one for each frame received on this port with the FCSError and FramingError signals asserted and CollisionEvent signal deasserted and whose OctetCount is greater than or equal to minFrameSize and less than or equal to maxFrameSize (Ref: IEEE 802.3 Std, 4.4.2.1). If rptrMonitorPortAlignmentErrors is incremented then the rptrMonitorPortFCSErrors Counter shall not be incremented for the same frame.

Frame Too Longs - This counter is incremented by one for each frame received on this port whose OctetCount is greater than maxFrameSize (Ref: 4.4.2.1, IEEE 802.3 Std). If rptrMonitorPortFrameTooLongs is incremented then neither the rptrMonitorPortAlignmentErrors nor the rptrMonitorPortFCSErrors counter shall be incremented for the frame.

Short Events - This counter is incremented by one for each CarrierEvent on this port with ActivityDuration less than ShortEventMaxTime. ShortEventMaxTime is greater than 74 bit times and less than 82 bit times. ShortEventMaxTime has tolerances included to provide for circuit losses between a conformance test point at the AUI and the measurement point within the state machine.

Runts - This counter is incremented by one for each CarrierEvent on this port that meets one of the following two conditions. Only one test need be made. a) The ActivityDuration is greater than ShortEventMaxTime and less than ValidPacketMinTime and the CollisionEvent signal is deasserted. b) The OctetCount is less than 64, the ActivityDuration is greater than ShortEventMaxTime and the CollisionEvent signal is deasserted. ValidPacketMinTime is greater than or equal to 552 bit times and less than 565 bit times.

Runts usually indicate collision fragments, a normal network event. In certain situations associated with large diameter networks a percentage of collision fragments may exceed ValidPacketMinTime.

Collisions - This counter is incremented by one for any CarrierEvent signal on any port for which the CollisionEvent signal on this port is also asserted.

Late Events - This counter is incremented by one for each CarrierEvent on this port in which the CollIn(X) variable transitions to the value SQE (Ref: 9.6.6.2, IEEE 802.3 Std) while the ActivityDuration is greater than the LateEventThreshold. Such a CarrierEvent is counted twice, as both a collision and as a lateEvent.

The LateEventThreshold is greater than 480 bit times and less than 565 bit times. LateEventThreshold has tolerances included to permit an implementation to build a single threshold to serve as both the LateEventThreshold and ValidPacketMinTime threshold.

Very Long Events - This counter is incremented by one for each CarrierEvent on this port whose ActivityDuration is greater than the MAU Jabber Lockup Protection timer TW3 (Ref: 9.6.1 & 9.6.5, IEEE 802.3 Std). Other counters may be incremented as appropriate.

Data Rate Mismatches - This counter is incremented by one for each frame received on this port that meets all of the following conditions: a) The CollisionEvent signal is not asserted. b) The ActivityDuration is greater than ValidPacketMinTime. c) The frequency (data rate) is mismatched from the local transmit frequency. The exact degree of mismatch is vendor specific and is to be defined by the vendor for conformance testing.

When this event occurs, other counters whose increment conditions were satisfied may or may not also be incremented, at the implementor's discretion. Whether or not the repeater was able to maintain data integrity is beyond the scope of this standard.

Auto Partitions - This counter is incremented by one for each time the repeater has automatically partitioned this port. The conditions that cause port partitioning are specified in the partition state machine in Section 9 [IEEE 802.3 Std]. They are not differentiated here.

Total Errors - The total number of errors which have occurred on this port. This counter is the summation of the values of other error counters (for the same port).

Creating a Static Route

To add a static route, enter the new route information listed below in the IP Routing Information dialog box. Then click on the Add button.

Destination Address — Enter the destination address for the current entry.

Subnet Mask — Enter the network mask for the current entry.

Next Hop — Enter the next hop for the current entry.

Routing Type — Enter the basic type of routing for this entry. The options include *Direct*, *Indirect*, *Invalid*, and *Remote*.

Interface Identifier — Enter the interface ID through which the next hop should be reached.

Routing Metric1 — Enter the primary routing metric for this entry.

Protocol Information

IPX Basic System Information

This dialog lists basic IPX system information. Each instance that IPX runs on the router will be displayed. The entire IPX network is displayed in list form on this dialog. You may select any entry from this list to display the full system information for the selected entry. The dialog automatically lists the first entry in the list until another entry is selected. The following information is listed on this dialog:

Name — The name of the current IPX system entry.

Instance — The IPX Instance ID is a unique identifier of the instance of IPX to which this row corresponds. This value may be written only when creating a new entry in the table.

Network Number — The network number section of the IPX address.

Node Number — The node number section of the IPX address.

Status — The validity for the current IPX system table is represented in this field. Setting this field to Off indicates that this entry may be deleted from the system table at the IPX implementation's discretion.

Socket Open Fails — The number of IPX packets discarded because the destination socket was not open.

Max Sockets — The maximum number of IPX sockets that may be open at a time.

Refresh — Updates the values in each field.

Statistics — Select this button to view the IPX Basic System Stats dialog.

Circuits — Select this button to view the IPX Circuits dialog.

IPX Routing Destinations

This dialog contains information about all known destinations. The routing information shown in this table represents the path currently being used to reach the destination. Each entry corresponds to one destination.

IPX Instance (ipxDestSysInstance) — The unique identifier of the instance of IPX to which this row corresponds.

Dest Net Number (ipxDestNetNum) — NetNumber. The IPX network number of the destination.

Dest Protocol (ipxDestProtocol) — Values: other(1), local(2), rip(3), nlsp(4), static(5). The routing protocol from which knowledge of this destination was obtained.

Delay Ticks (ipxDestTicks) — The delay in ticks to reach this destination.

Hop Count (ipxDestHopCount) — The number of hops necessary to reach the destination.

Next Hop Circuit ID (ipxDestNextHopCircIndex) — The unique identifier of the circuit used to reach the next hop.

Next Hop NIC Address (ipxDestNextHopNICAddress) — PhysAddress. The NIC address of the next hop.

Next Hop Network (ipxDestNextHopNetNum) — NetNumber. The IPX network number of the next hop.

Refresh — Updates the values in each field.

Static Routes — Opens the Static Routes dialog.

IPX Services

This table contains the services information, indexed by service name and type. Each entry corresponds to one service.

IPX Instance (ipxServSysInstance) — The unique identifier of the instance of IPX to which this entry corresponds.

Service Name (ipxServName) — Octet string. The service name.

Service ID (ipxServSocket) — Octet string. The socket portion of the IPX address of the service.

Hop Count (ipxServHopCount) — The number of hops to the service.

Service Type (ipxServType) — Octet string. The service type.

Service Protocol (ipxServProtocol) — Values: other(1), local(2), nlsp(4), static(5), sap(6). The protocol from which knowledge of this service was obtained.

Network Number (ipxServNetNum) —NetNumber. The IPX network number portion of the IPX address of the service.

Node Address (ipxServNode) — Octet string. The node portion of the IPX address of the service.

Refresh — Updates the values in each field.

IPX Circuits

This dialog contains the IPX circuit management information and can be viewed in two ways. The first is by available IPX circuits on the router, and the second is by all circuits for an IPX Instance as found in the Basic IPX list. The following information fields are displayed:

Name — The readable name for the circuit.

Dial Name — This symbolic name is used to reference the dialing used to create this circuit. This value may be written only when creating a new entry.

IPX Instance — The unique identifier of the instance of IPX for this entry. This value may be written only when creating a new entry.

Circuit Identifier — The identifier for this circuit that is unique within the instance of IPX. This value may be written only when creating a new entry.

Operational State — The operational status of this circuit.

Existence Status — The validity for this circuit entry. A circuit with this field set to Off may be deleted.

Interface Identifier — Lists the interface that IPX is running on in this instance.

Circuit Type — The type of circuit.

Max Packet Size — The maximum size in bytes supported for this circuit.

Route Status — Indicates whether the information about static routes services read through this circuit matches those saved in permanent storage. Setting the value to Write when the value changed will write the “currently in use” information to permanent storage. Setting the value to Read when the value changed will replace any routes and services currently defined for the circuit with those read from permanent storage.

Refresh — Updates the values in each field.

Compression Stats — Displays the IPX Compression Stats dialog.

Circuit Info — Displays the IPX Circuit Information dialog.

IP Statistic Information

This dialog contains the basic IP counters and other statistical information about the IP protocol functioning on this device. This includes counters for the errors as well as input and output statistics. You have the ability to reset the counters from this dialog. Following are the variables that are included on this dialog:

Forwarding Status — This parameter is enabled if the device is acting as a gateway.

Packets Received — The total number of IP input datagrams received.

Output Requests — The total number of IP datagrams the local IP user-protocols supplied to IP in request for transmission. Note that this counter does not include any datagrams counted in the Packets Forwarded field.

Delivered Packets — The number of datagrams delivered to IP user-protocols.

Packets Forwarded — The number of IP datagrams forwarded.

Fragments Reassembled — The number of IP datagrams successfully re-assembled.

Fragments Created — The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Fragments Received — The number of IP fragments received that required re-assembly at this entity.

Packets Fragmented OK — The number of IP datagrams that have been successfully fragmented at this entity.

Re-assembly Timeout — The maximum period in seconds that received fragments are held while they are awaiting re-assembly at this entity.

Default Time to Live — The default value inserted into the time to live field of the IP header for datagrams originated at this device.

Addressing Errors — The number of datagrams discarded because the destination IP address in the packet was not valid for this device.

Input Header Errors — The number of datagrams discarded due to IP header errors.

Discarded Packets — The number of datagrams discarded because the destination IP address in the packet was not valid for this device.

Re-assembly Failures — The number of failures detected by the IP re-assembly algorithm for any reason (timed out, errors, etc.). This is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.

Unknown Protocols — The number of discarded datagrams due to unsupported protocols on this device.

Fragmentation Failures — The number of IP datagrams that have been discarded because they required fragmentation at this entity but could not be fragmented.

Num Route Discards — The number of datagrams discarded due to no route.

Refresh — Updates the values in each field.

Reset Counters — Resets the counters values to 0.

Routing —Displays the IP Routing Information dialog.

Addresses — Displays the IP Address Mapping dialog.

Options\Polling Setup — Opens the Polling ParameterSetup dialog, where you can specify how you want the parameter dialog to refresh.

IP Address Resolution

This dialog comprises the IP Address translation table, used for mapping IP addresses to physical addresses. Each entry contains one IP Address to “physical” address equivalence.

MAC Address (ipNetToMediaPhysAddress) — The media-dependent 'physical' address.

IP Address (ipNetToMediaNetAddress) — The IP Address corresponding to the media- dependent 'physical' address.

Interface ID (ipNetToMediaIfIndex) — The interface on which this entry's equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Arp Type (ipNetToMediaType) — The type of mapping: Invalid(2), Dynamic(3), Static(4), and Other(1). Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the Table. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant Type object.

Refresh — Updates the values in each field.

X.25 Protocol Information

This dialog lists all of the X.25 interfaces on the device. From this dialog you can access operational information, timer information, and statistics. The following buttons are displayed:

Operational Information — Displays the X.25 Operational Information dialog where you can view information about the operation of the selected X.25 interface.

Timer Information — Displays the X.25 Timer Information dialog where you can view timer description, value, and count for the selected X.25 interface.

Statistics — Displays the X.25 Interface Statistics dialog where you can view information on the statistical counters of the selected X.25 interface.

Refresh — Updates this dialog.

ISDN Protocol Information

This dialog allows you access to the other ISDN information dialogs. The following buttons are available:

Line Configuration — Displays the ISDN Line Configuration Details dialog.

Versions — Displays the ISDN Interface Version Information dialog.

Refresh — Updates the values on this dialog.

Frame Relay Interface Information

This dialog contains a list of all Frame Relay interfaces on the current device. You can launch any of the other detailed Frame Relay dialogs from this dialog:

Data Link — Displays the Frame Relay Data Link Connection Management dialog where you can view data link connection management information.

Virtual Circuit — Displays the Frame Relay Virtual Circuits dialog.

Errors — Displays error statistics for the currently selected Frame Relay interface.

Refresh — Updates the values on this dialog.

PPP Protocol Information

This dialog lists all of the point-to-point (PPP) interfaces on this device and allows you to view information on the following topics:

Link Status — Displays the PPP Link Status Information dialog with the current information on this PPP link.

Link Quality — Select *Link Quality* to go the PPP Link Quality dialog for information on a link where LQR monitoring has successfully been negotiated for the link.

IP Status — For information on PPP IP network protocol for this selected PPP interface, select this button.

Bridging — To view bridging parameters that are related to bridging over the PPP interface, select the *Bridging* button.

Refresh — Updates the values on this dialog.

Ethernet Interface Information

This dialog contains a list of all the Ethernet interfaces on the current device. You have the following options from this dialog:

Errors — Displays the Ethernet Errors dialog.

Refresh — Updates this dialog.

Token Ring Interfaces

This dialog contains a list of all the Token Ring interfaces on the current device. You have the following options from this dialog:

Configuration — Opens the Token Ring Configuration dialog.

Timers — Opens the Token Ring Timers dialog.

Errors — Opens the Token Ring Error Statistics dialog.

Refresh — Updates the interfaces displayed on this dialog.

Working With Graphs

Netelligent Management Software provide a sophisticated graphing function that lets you view a variety of device- and port-level statistics in real time. You can view graphs on screen, print graphs, or export them to a file.

Starting the Graphing Function

To graph port utilization, input, and output statistics, follow these steps:

1. Click on *SNMP Statistics/Interfaces* to display the Device Interface List. The Graphing menu appears on the main window menu bar.
2. Click on an interface from the Device Interface List.
3. Click on the Graphing menu and select a port utilization or input/output graphing option to view the main graphing window.

To graph detailed statistics for a device, follow these steps:

1. Display the device's graphical interface by double-clicking on the device icon.
2. Display a statistics window for the device.
3. Click on the Graphing menu from the main menu bar or right-click on any numerical display in a statistics window to view the graphing popup menu.
4. Select the desired option to start graphing.

Setting Graph Thresholds

The graphing function lets you set thresholds on monitored data on a per graph basis. If the graph is monitoring multiple statistics, you must specify which set of data the threshold applies to. See "Starting the Graphing Function."

To set the thresholds for a particular graph, click on *Thresholds* from the main graph window to display the Thresholds dialog box.

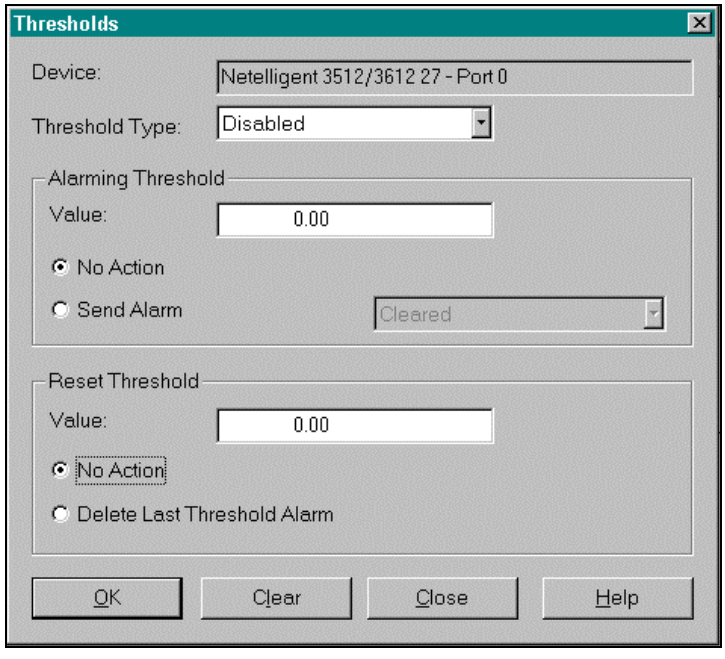


Figure 2- 10. Thresholds Dialog Box

Setting the Threshold Type

You can select from three available threshold options, including Disabled, Falling Threshold, and Raising Threshold.

Select *Disabled* if you prefer no thresholds during graphing.

Select *Falling Threshold* if you want certain events to occur when a data point on the graph falls below the designated value.

Select *Raising Threshold* if you want certain events to occur when a data point on the graph goes above the designated value.

Setting the Alarming and Reset Thresholds

The Alarming and Reset Threshold areas let you set a specific threshold value at which time the software generates an alarm, deletes the last threshold alarm, or performs no action when the threshold is reached.

After you select a threshold type, enter the desired threshold value in the Value fields. Then select the action that you want to occur when the graphed value rises above or falls below the entered values.

If you select *Send Alarm*, click on the drop-down menu to the right of this option and select the type of alarm you want the software to send.

The software sends an alarm when the graphed value exceeds the rising threshold value. Then, after the graphed value falls below the falling threshold value, the software sends a clear alarm.

Click on *Clear* to clear the fields and return them to their default values.

NOTE: If the system is shut down, the software does not retain the threshold alarming state.

Hiding a Graph

You can hide a graph if you prefer not to display the graph window. To hide the graph, click Hide on the main graphing window. The software continues to graph data. To redisplay the graph, select *Tools/Running Graphs* to display the currently running graphs. Then select the desired graph and click on *Show Graph*.

Printing a Graph

To print a graph, click on *Print* from the main graphing window. The standard Windows 95 Print dialog box appears. Select the desired options and click on *OK*.

Exporting Graph Data to a File

The Auto Export tab of the Graph Properties dialog box lets you export monitored graph data to a text file for later analysis. The exported data includes the calculated values and the system time they were graphed. The Auto Export function provides the following two options:

No Auto Export — Performs no export function

Continuous Export — Continuously appends the file that the data is exported to.

Delimiter — This option is active if you select *Continuous Export*. Select the preferred delimiter (field separator) to allow you to import the data file into another program, such as a database application.

Filename — Click on the button next to this field name to display the Select Export File Name dialog box. Enter the desired filename and directory. Then click on *Open*. The selected filename appears on the Filename button.

Viewing Running Graphs

You can display all currently running graphs by selecting View Running Graphs from the Network menu. When you select this option, the following window appears:

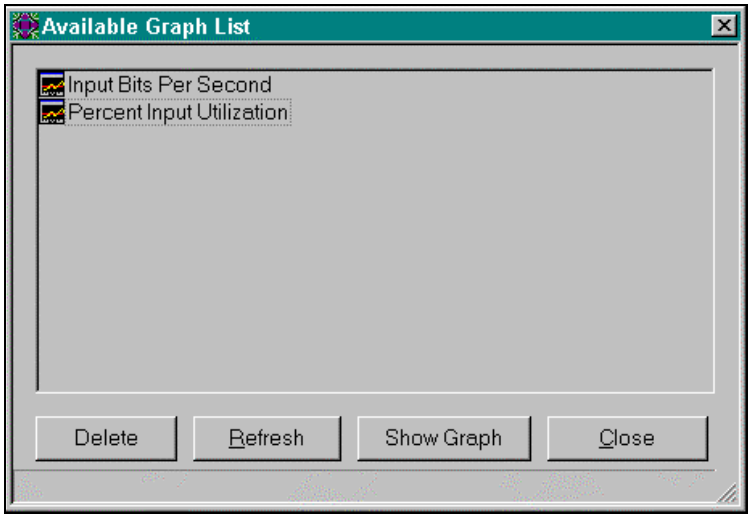


Figure 2- 11. Viewing Running Graphs

Delete — Deletes the selected graph

Refresh — Refreshes the data display for the selected graph

Show Graph — Displays the selected graph if the graph is hidden

Setting Graph Polling Options

The Polling tab of the Graph Properties dialog box displays the following information:

Poll Every … Seconds — The interval of time, in seconds, between polls. Enter a value from 1 to 3600.

Points on Graph — The maximum allowed number of data points displayed on the graph. Select a value from 10 to 1000 by entering the value in the data field or by moving the slide control to display the desired value.

Number of Responses — Displays the number of polling responses (data samples) that are included on the graph.

Time Started — Shows the day, hour, minute, and second that the graph started.

Selecting Graph Styles

The Styles tab of the Graph Properties dialog box lets you change the way data is represented on the main graphing window. It provides the following options:

Line Graph — Displays data as a single line

Bar Chart — Displays data as a series of vertical bars

Area Graph — Similar to a line graph, this format displays data as a solid area with the line graph as the top boundary of the data display.

Log Scale — Check this option to change the measurement scale (Y-axis).

Invert Data — Check this option to switch the X-axis time data with the Y-axis measurement scale.

X - Grid Lines — Check this option to display vertical grid lines above the X-axis time entries.

Y – Grid Lines — Check this option to display horizontal grid lines along the scale marks.

Setting Graph Colors

The Colors and Lines tabs of the Graph Properties dialog box let you change the colors of the main graphing window components.

Changing the Background and Text Color

To change the color of the graph main background, text, or title background, follow these steps:

1. Click on the button for the area you want to change.

2. Select the desired color from the standard Windows 95 color palette and click on *OK*.
3. Click on *Apply* to change the color on the display and click on *OK*.
4. Click on *Save Default Colors* to save the selected colors as the default settings.

Changing the Line and Point Color

To change the color of the graph line and data points, follow these steps:

1. Click on the button for the area you want to change.
2. Select the desired color from the standard Windows 95 color palette and click on *OK*.
3. Click on *Apply* to change the color on the display and click on *OK*.
4. Click on *Show Points* to display the data sampling points on the graph.
5. Click on *Save Default Colors* to save the selected colors as the default settings.

Using the Compaq Common MIB

This section discusses functions available for Netelligent devices that support the Compaq common MIB.

Compaq Devices Information

Netelligent Management Software supports the Compaq MIB for certain Netelligent products. To access information about Compaq devices and the Compaq MIB, follow these steps:

Select *Edit/SNMP Statistics/Protocols*, or select *SNMP Statistics/Protocols* from the device right-click menu. If the device supports the Compaq MIB, the Compaq button should be active (non-grayed). Click on the *Compaq* button to display the Compaq Devices Information dialog box.

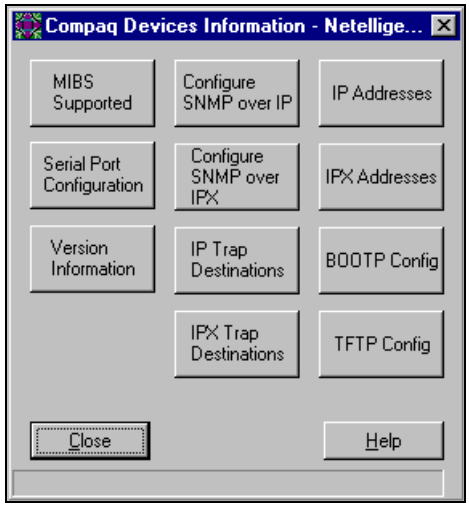


Figure 2- 12. Compaq Devices Information Selection Box

Supported MIB Modules

The Supported MIB Modules dialog box displays each of the MIB modules the device supports.

Module Description — A textual description of the supported MIB module for the selected entry.

Object ID — The SNMP OID equivalent for the current entry. If possible, the MIB object names are used in place of the identifiers.

Setting SNMP and IP Access

The SNMP IP (or IPX) Community Access Configuration dialog box lets you control SNMP access into a device.

You can delete any entry displayed or add a new entry. To delete an entry, highlight the entry and click on *Delete*. To add a new entry, enter the required information in the upper section of the dialog box and click on *Add*.

Community Name — The community string that is required for any requests coming from this host

Entry ID — A unique identifier for the entry

IP Address — The masked IP (IPX) address

Address Mask — This mask is applied to the source address of received SNMP/IP messages. If the masked address matches the IP address (IPX address) object and the community in the SNMP packet matches the community name for the row, then the SNMP request will be serviced by the device's agent.

Access Level — This object controls the access granted to SNMP requests which match a mask/match and community string name. Available options are *No Access*; *Read Only, No Telnet*; and *Read Write*, *Enable Telnet*.

Configuring an IP Address

The IP Address Configuration dialog box lets you view and modify all the current interfaces that support IP addressing. Click on Apply after you make the desired changes.

Interface ID — The ifIndex value of an interface in the MIB-II interface table for which this table entry applies (read-only)

IP Address — The IP address of this agent interface

Default Route — The address of the next hop router (gateway) used by this interface

Hardware Address — The physical address of the management agent interface. This is equivalent to the MAC Address (read-only)

IP Network Mask — The IP subnet mask of this agent interface

Frame Type — Except when booting up, an agent communicates over IP using a single frame type defining the type of network that the IP traffic is running on. The two available options are Ethernet_II and IEEE 802.2_SNAP.

Auto Discover State — Lets you enable the device to send out periodic ICMP pings to ensure that the device's IP Address is contained in the ARP cache of its default gateway (if one exists).

Ping Rate — Determines the rate (in seconds) at which ICMP pings are sent out by the device to ensure that its IP address remains in the ARP cache of the device's default gateway.

Saving the IP Address Configuration

If you make changes to the IP address configuration, click on *Commit to NVRAM* to save the new settings. If there have been no changes to the currently selected entry, this button is grayed out.

Configuring an IPX Address

The IPX Address Configuration dialog box you view and modify all the current interfaces that support IPX addressing. You can modify the frame type or broadcast status. Click on Apply to apply the changes to the selected device.

Interface ID — The ifIndex value of an interface in the MIB-II interface table for which this table entry applies

Hardware Address — The physical address of the management agent interface. This is equivalent to the MAC address.

IPX Address — The IPX address of this agent interface

IPX Frame Type — The frame type the device uses for IPX communication

Generate SAP Broadcasts — The device may generate IPX SAP broadcasts. Enabling this option allows the device to be auto-discovered.

Configuring a Serial Port

The Serial Port Configuration dialog box lets you configure the serial ports for modem or terminal communications.

The dialog box uses the following MIB objects to configure the serial port:

Primary Serial Port — The entry in the cpqnSerialPortTable MIB object designated as the primary serial port

Selected Serial Port — The unique key for the table

Selected Interface — The value of the corresponding index entry in the interface table

Enable Modem Init String — Click on *Yes* to enable or click on *No* to disable the transmission of the modem initialization string defined by cpqnSPortModemInitString MIB object out of the serial port.

Modem Initialization String — The modem initialization string that will be sent if the cpqnSPortModemInitStringEnable object is set to enable.

Auto Detect Baud — Click on *Enable* to enable automatic baud detection. If this option is enabled, it may change the baud rate on the agent. Click on *Disable* to disable automatic baud detection.

Baud Rate — The current baud rate for the port. This value must match a cpqnBaudRate entry in cpqnSupportBaudRateTable. This value could automatically change if the cpqnSPortModemAutoNegotiateState MIB object is set to Enabled. This field also displays a list of available baud rates.

Viewing Component Version Information

The Component Version Information dialog box displays read-only information about the device's software and hardware.

Description — A brief description of the component. This field may be empty.

Serial Number — The serial number of this component. The format of this field depends on the device type. This field is empty for components that do not have a serial number.

Revision — The revision of the step for the associated component. For example, V1.0B3 indicates revision three of the beta version of a component.

Entry ID — A number that uniquely identifies which device in a group of one or more devices that this entry applies to.

Parent Entry — A number that uniquely identifies an entity or device of which the entries in this table may be a sub-component.

Component ID — A number that uniquely identifies which component of a device this entry applies to.

Component Type — The component's type (Hardware or Software)

Setting IP and IPX Trap Destinations

The IP and IPX Trap Destination dialog boxes let you modify or delete existing trap destination entries and add new entries.

Entry ID — A number that uniquely identifies which device in a group of one or more devices that this entry applies to.

Community Name — A community to which this destination address belongs. You cannot modify this object if the associated trapIPDestStatus MIB object is set to valid(1).

Destination Address — The address to send traps on behalf of this entry

To add a new entry, enter the information in the Community Name and Destination Address fields and click on *Add*. To modify existing entries, select the entry, modify the information, and click on *Apply*. To delete an entry, select the entry and click on *Delete*.

Configuring BootP

The BOOTP Configuration dialog box lets you configure BOOTP for each interface that supports the BOOTP protocol. The window shows a list of all these interfaces and their current BOOTP configuration status.

Interface ID — The ifIndex value of an interface in the MIB-II interface table for which this table entry applies

Server IP — The IP address of the BOOTP server that last responded on the interface indicated by the cpqnBootpifIndex MIB object. If no BOOTP server has responded, this value will be 0.0.0.0.

Request State — This selection menu lets you enable or disable the generation of BOOTP requests on the interface specified by the cpqnBootpIfIndex MIB object. BOOTP requests can be generated over the SNAP frame type, Ethernet-II frame type, or both.

Number Retries — The number of BOOTP requests that will be transmitted from the interface indicated by the cpqnBootpifIndex MIB object

Retry Interval — The time period (in seconds) between the transmission of BOOTP requests on the interface specified by the cpqnBootpifIndex object

Configuring TFTP

The TFTP Configuration dialog box provides options that let you configure a TFTP server. The box also displays any error information that pertains the TFTP transfers.

Desired Transfer Status — Provides TFTP transfer status options. Select *Initiate Transfer* to initiate a TFTP download/upload of the all files set to download/upload in the cpqnTftpTransferState MIB object.

Enable File Transfer Traps — Select *Enabled* to enable sending TFTP file transfer traps.

File Name — The fully qualified path and filename of the file to download or upload

Type of File — The type of file that this entry represents. Options include *Agent Software*, *ATM Uplink Firmware*, and *Booter*.

Current Transfer Status — Determines the current TFTP file transfer status. Selecting *Download File, when initiated* when the Desired Transfer Status field (cpqnTftpInitiate) is *Initiate Transfer* will download the file associated with this entry from the server specified by the cpqnTftpServerIp MIB object.

File Version — The version of file to be downloaded

IP Address of Server — The IP address of the TFTP server

Most Recent Transfer Error — The error status (if any) of the last upload or download that occurred for this entry

Error Description — A description of any additional error information that is not fully handled by the cpqnTftpTransferLastErr object.

NOTE: The Desired Transfer Status and Current Transfer Status fields must be set to initiate and download files, respectively.

Using Netelligent Management Software Utilities

Netelligent Management Software provides numerous utilites that facilitate device and map management.

Configuring a BootP Server

When network devices capable of BootP are powered up, they send a BootP request over the network. This request includes the MAC address of the requesting device. When BootP servers receive these requests over the network, they compare the MAC address in the request with a list of addresses in the Bootptab (BootP table). The Bootptab record contains an IP address, IP mask, and a configuration file name for each MAC address. If a MAC address match is found, the server sends the IP address and name of the configuration file to the requesting device.

Follow these steps to configure your workstation as a BootP server and enable it to handle BootP requests.

1. Create a network map and configure all devices on the map.
2. Select Network/Bootptab Maintenance.

Note: The configuration files used must be kept in the directory where Compaq Netelligent Management Software is installed. By default, this would be C:\Netmgr.

Use this window to map IP addresses to MAC (physical) addresses of network devices and to associate a configuration file with the device. Enter the information as follows:

MAC Address — Enter the unique MAC address of the network device.

IP Address — Enter the IP address to be assigned to the network device.

IP Mask — Enter the IP subnet mask for the IP address to be assigned.

Gateway — Enter the IP gateway for the device.

Boot File — Enter the name of the boot file to be sent to this device. The configuration files must remain in the directory where the Netelligent Management Software is installed (C:\NETMGR, for example).

Configured Devices Available — This area shows a list of all devices on the current map for which a configuration file has been created.

Serviced — This checkbox is checked for the selected MAC address if the software has responded to a requesting device.

Enabling BootP

BootP (bootstrap protocol) allows unconfigured devices to obtain information such as an IP address, subnet mask, gateway router, configuration file, and other vendor-specific information. Netelligent Management Software comes with a built-in BootP/TFTP server.

To enable the BootP server, select *Network/BootP Server/Enabled*.

Setting Up Health Polling

To set up health polling for individual devices, follow these steps.

1. Right click on a device icon on a network map to display the device menu and select *Properties*. The Device Properties window appears.
2. Select the Health Polling tab.
3. Enable health polling.
4. Set the polling time interval (1 second minimum) if necessary.
5. Select the type of alarm you want the software to send.

   Informational

   Indeterminate

   Minor

   Major

Critical

6. Click on *OK*.

NOTE: Setting a shorter polling interval provides a more up-to-date status for a device, but it also increases traffic on the network.

Enabling Health Polling

Health polling verifies that an SNMP manageable device is responding normally. If a device fails to respond within a predefined interval, the software logs an error. In the Network Workspace window, the icon for any polled device that fails to respond normally displays the color you selected for the device status of the alarm. If the device responds normally to the poll, any previous poll failure will be cleared.

To enable health polling for all devices on the map, select *Network/Health Polling/Enable*. Health polling is automatically enabled when you start Netelligent Management Software.

Changing the Color for Device Status

The Device Status legend lets you change the icon background color of any alarm event. Select *Window/Device Status Legend* to display the following window:

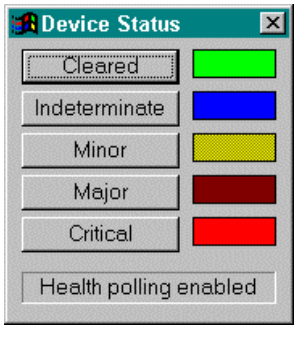


Figure 2- 13. Device Status Legend

This window identifies the colors that represent the results of the latest Health Poll. The possible results are as follows:

Cleared - default color is green. This indicates that the network device responded to the last health poll.

Indeterminate – default color is blue. This indicates the device is not being polled because it has not been configured for health polling or has not been configured with an IP address.

Minor – default color is gold. This indicates a minor error condition.

Major – default color is brown. This indicates a major error condition.

Critical - default color is red. This indicates a severe error condition, such as a failed health poll.

To change a default color on the legend, click on the button next to any color. Then select the desired color from the standard Windows 95 color palette and click on *OK* to apply the new color.

Pinging All IP Addresses

To ping all IP addresses of the devices in your network, select *Network/Ping all IP addresses*. The software launches the Windows 95 MS-DOS application. It then pings each device and displays the results in the MS-DOS window. The length of time this process takes to complete depends on the number of IP addresses on the network.

Determining a Device Type

Select *Edit/SNMP Verify* to query a device to determine what type of device it is. The software obtains the device's sysObjectID and sysServices information. If it can determine the type of device, it changes the icon on the network map to reflect the device type and logs any pertinent information related to the device.

Changing a Mapped Device Type

To change the device type for a mapped device, select *Utilities/Change Device Type* from the device right-click menu. Select the new device type from the list of devices and click on *OK*. After you select the new device type, the software automatically reassigns the old device's circuits to the new device.

Showing State Colors

To enable the map to display the status color of object icons, select *Network/Show State Colors/Enabled*. To turn off the color for the icons, select *Network/Show State Colors/Disabled*.

Enabling TFTP

Netelligent Management Software supports the TFTP protocol for transferring and receiving files. To enable or disable the configuration workstation as a TFTP server, select *Network/TFTP Server*.

Making TFTP Transfers

The TFTP file transfer function lets you transfer files to or retrieve files from a network device using the TFTP protocol.

Select *Network/TFTP File Transfers*. In the resulting dialog box, select the *Get* button to receive a file from the network device or select the *Put* button to send a file from the workstation. You can transfer files in a binary or text mode. Enter the filename you want to send or receive and enter the IP address for the device that will send or receive the file.

Starting the MIB Browser

To start the Netelligent MIB Browser, click on the MIB Browser button from the button bar, or select *SNMP Statistics/MIB Browser* from the device right-click menu.

Compacting the ODBC Database

Follow these steps to compact the ODBC database in Netelligent Management Software:

1. Close Netelligent Management Software.
2. Open the Windows Control Panel.
3. Double-click on the ODBC icon to display the ODBC Data Source Administrator dialog box.

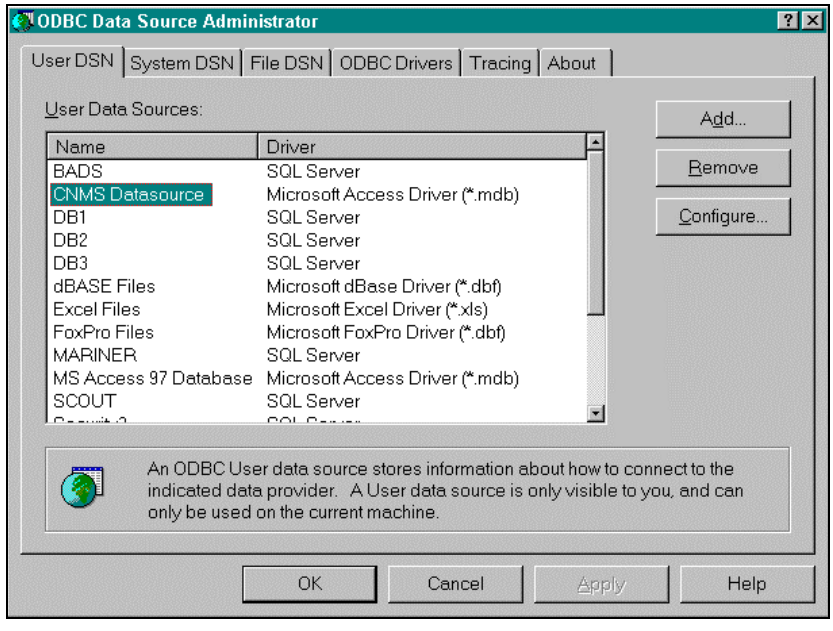


Figure 2- 14. ODBC Data Source Administrator Window

4. Select the User DSN tab and highlight *CNMS Datasource* from the User Data Sources area. An ODBC user data source stores information about how to connect to the indicated data provider. It is visible only to you and can be used only on the current machine.
5. Click on *Configure* to display the ODBC Setup dialog box.

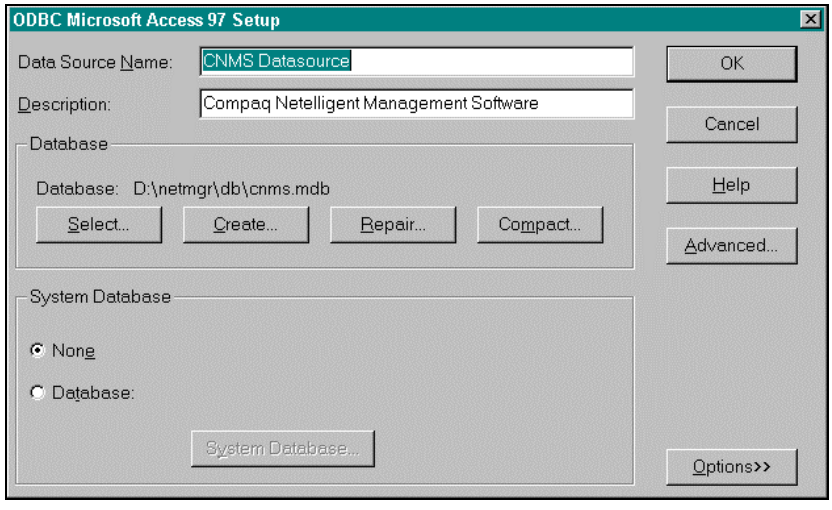


Figure 2- 15. ODBC Setup Window

6. Click on *Compact* to display the Database to Compact From dialog box.
7. Click on *OK* to display the Database to Compact Into dialog box.
8. Click on *OK*. A confirmation box states that the file you are trying to compact already exists and gives you the option of replacing the file.
9. Click on *Yes* to replace the old file.
10. When you receive a message that the compact operation is complete, click on *OK*.
11. Click on *OK* on each remaining window to return to the Control Panel. Then close the Control Panel.

Using the Event Log Viewer

Netelligent Management Software provides an Event Log Viewer which displays all event information that is being generated. The Event Log Viewer is pre-configured to show you most of the events in the event log. However, you can set up filters that show only the events that meet a certain criteria that you determine, thus limiting the number of events that appear in the viewer. The default number of events displayed is 5000, but you can set your own maximum values.

The Event Log Viewer displays the following information about events that occur while managing your network:

Event ID — A unique ID associated with this event.

Date/Time — The date and time the software received the event (not necessarily the date and time the event actually occurred)

Device Name — The name of the device that produced the event. Netelligent Management Software has a special "Management Console" pseudo-device associated with its console. Although there is no icon on the Network Devices window for the Management Console, this pseudo-device appears in the Event Log entries.

Event Class — The type of event that is being logged. Possible types are BOOTP, TFTP, Upload, Device Changed, System Information, Alarm Cleared, Equipment Alarm, Software Alarm, Threshold Alarm, Trap Alarm, and Health Polling Alarm.

Severity – In the case of an alarm, this is the severity of that alarm. If the event is not an alarm, this column is blank. The possible severity conditions of an alarm are: Cleared, Informational, Indeterminate, Minor, Major, and Critical.

State – This is the current state of an alarm. If the alarm has not been cleared or if the event is not an alarm, this field is blank. If the event is an alarm and if that alarm is cleared, this field contains the number of the event that caused the alarm to clear.

Information – The detailed description of the event.

Buttons along the bottom of the Event Log Viewer let you perform various functions in theEvent Log Viewer.

Click on *Filters* to filter out information you do not want to view in the Event Log Viewer. The filtered events still remain in the event log database.

Click on *Export* to export a log report as a text file for later reference.

Click on *Details* to view details about a specific log entry.

Click on *Clear Alarms* to clear selected alarms from the event log. The Event Log Viewer generates Alarm Cleared events for each of those selected events and updates the device state accordingly.

Setting Event Log Viewer Filters

The Event Log Viewer Filter Settings dialog box provides a way to filter out events you do not want to view in the Event Log Viewer. You can filter events using the following criteria:

- Device Name
- Event Class
- Alarm Severity
- Alarm State
- Start Date and Stop Date

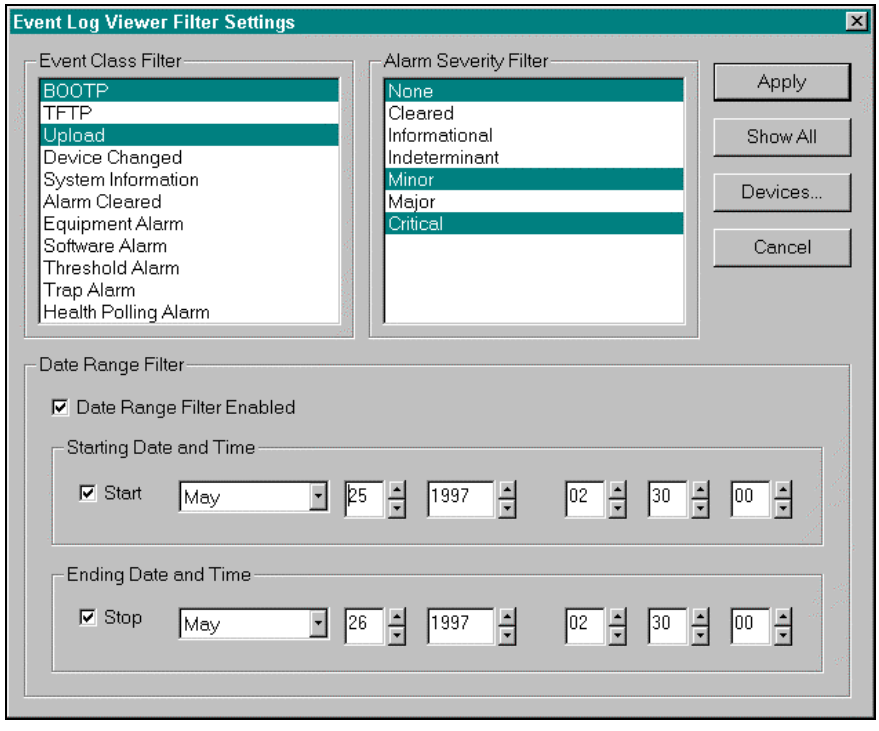


Figure 2- 16. Event Log Viewer Filter Settings Window

Event Class Filtering

Select all of the event class types for which you would like to see events. For example, if you wanted to see all event class types except those related to BOOTP or TFTP transfers, you would select all event class options except the BOOTP and TFTP entries.

NOTE: Some of the event classes are alarms. The Alarm Severity filter settings apply only to the selected alarm events.

Alarm Severity Filtering

Select all of the alarm severity conditions for which you would like to see events. The None and Cleared options are not alarm severity conditions, but rather are alarm *states*. To see events that are not alarms, be sure you select *None*. To see alarms, even after they have been marked as cleared, select *Cleared*. If you created an Event Log Viewer Filter that had all Event Classes except the Alarm Cleared option, and you selected all of the Alarm Filters except *None* and *Cleared*, you could view only Event Log entries of active alarms. Any alarm in that viewer that later clears would automatically disappear from the Event Log Viewer.

Alarm State Filtering

It is possible to filter alarms based on whether or not that alarm is still active. An alarm is considered active up until the time it is cleared by an Alarm Cleared event. To filter out cleared alarms, deselect the Cleared options under the Alarm Severity Filter box in the Event Log Viewer Filter Settings window.

Date/Time Filtering

You can select a start and/or stop time on which to filter events.

To see all Event Log entries that occurred prior to a particular time:

1. Enable the date range filter by clicking on the *Date Range Filter Enabled* checkbox.
2. Set the Stop date and time.
3. Disable the starting date and time by unchecking the checkbox next to the word *Start*.

To see only events that occurred within a certain time interval, set both a start and a stop date for the filter.

To see all events from the start time forward, set the starting date and time and disable the stop date and time.

Device Filtering

To select devices that correspond to the filtering attributes, click on *Devices*.

The resulting window displays the devices' descriptions, network addresses, types, and maps where they are located. You can select as many or as few devices as you want.

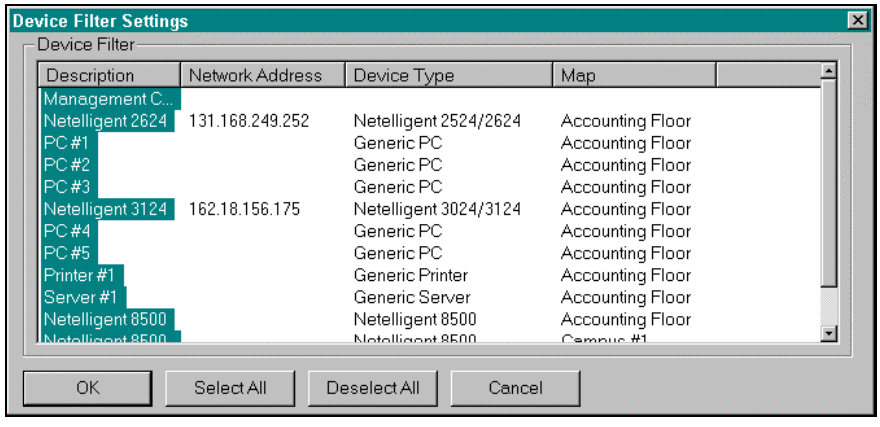


Figure 2- 17. Device Filter Settings Window

To select a single device, click on the device description.

To select multiple non-contiguous devices, press and hold down <Ctrl> and click on the device descriptions. To select a contiguous range of devices, click on the first device in the range, press and hold down <Shift>, and click on the last device in the range.

To select all devices, click on *Select All*. Or to deselect all devices, click on *Deselect All*.

Click on *OK* to close the dialog box and return to the Event Log Viewer Filter Settings window. After you apply the filter, only events related to the devices you selected appear in the Event Log Viewer. To display System Information type events that are related directly to Netelligent devices, select the Management Console device (at the top of the list).

Click on *Show All* to display all available events.

NOTES:

— The event log viewer only suppresses information from the event log display. It does not remove the information from the database.

— In the Event Log Viewer Filter Settings window, highlight the information you want to display. That is, do not highlight information you want to suppress from the event log viewer.

After you set all the filtering criteria, click on *Apply*. The Event Log Viewer reloads the matching events from the database.

Setting a Default Event Log Viewer Filter

You can set up a default event log filter that the software automatically applies to each Event Log Viewer window you open. To set the default filter, select *Tools/Preferences* to display the Properties dialog box. Then select the Event Log Viewer Filter tab.

Select the desired Event Class Filter(s) and Alarm Severity Filter(s). Then click on *OK*.

Exporting Event Log Entries

You can export to a text file the event log entries displayed in the Event Log Viewer or entries contained in the database.

Exporting Displayed Event Log Entries to a Text File

To export event log entries displayed in the Event Log Viewer to a text file, click on *Export* from the Event Log Viewer window to view the Export Settings dialog box.

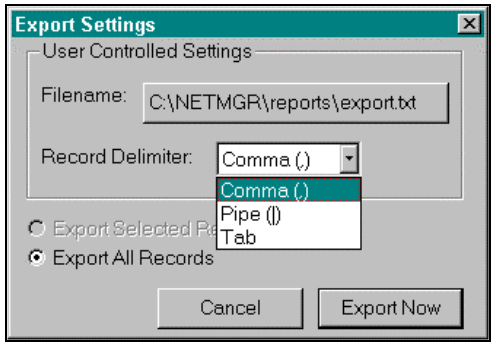


Figure 2- 18. Export Settings Window

Select the filename by clicking on the *Filename* button. The Export as… dialog box appears. Select the desired filename and directory and click on *Save*.

The Record Delimiter field lets you select a comma, pipe, or tab to delimit data in the file so that you can import the file into a spreadsheet or database program.

You can export selected records or all records in the event log viewer. Click on the desired option and click on *Export Now*. The software saves the data to a file in the selected directory.

Exporting and Removing Event Log Entries from the Database

The Database Export/Database Cleanup dialog box provides another way to export event log entries to a file based on filters you specify. This method lets you export more events than can be shown in an Event Log Viewer window. This dialog box also lets you permanently remove entries from the database.

Follow these steps to use the dialog's export and database functions:

1. Select *Tools/Export Log File* to display the Database Export/Database Cleanup dialog box.
2. Select the desired Event Class and Alarm Severity filters.
3. The checkboxes in the Database Export and Database Cleanup areas allow three different functions:

- Both boxes checked (default) — Exports the event log entries to a file and then automatically removes them from the database.
- Database Export checkbox only — Exports the event log entries to a file and retains all entries in the database.
- Database Cleanup checkbox only — Removes the event log entries from the database but does not export the entries to a file.

NOTE: If you remove entries from the event log database, the size of the database will not decrease until you compact the database. See "Compacting the ODBC Database."

4. Select device filters and date range filters as described below.
5. Click on *Continue*.

If you set the export function to permanently remove event log entries from the database, a confirmation box informs you that any removals are permanent and cannot be restored. Click on *OK* to remove the entries, or click on *Cancel* to continue with the export operation but retain the entries.

If you set the export function to export the event log entries to a file, the Export Settings dialog box lets you set the filename to which the software will save the entries. See "Exporting a Log Report."

Using the Device Filter

To select devices that correspond to the filtering attributes, click on *Devices*. The Export – Device Filter Setting window appears. This window displays the devices' descriptions, network addresses, types, and maps where they are located. You can select as many or as few devices as you want.

- To select a single device, click on the device description.
- To select multiple non-contiguous devices, press and hold down <Ctrl> and click on the device descriptions. To select a contiguous range of devices, click on the first device in the range, press and hold down <Shift>, and click on the last device in the range.
- To select all devices, click on *Select All*. Or to deselect all devices, click on *Deselect All*.

Click on *OK* after you have selected the desired devices.

Using the Date Range Filter

The date range filter lets you determine what events are exported based on the dates and times the events occurred. To enable the date range filter, click on the box next to Date Range Filter Enabled so that an X appears. Enter the desired dates and times in the Starting and Ending Date and Time fields.

Viewing Event Log Entry Details

To view details about a specific log entry, click on *Details* or double-click anywhere on the entry line. The Event Log Entry Details window appears. This window displays information in a more event specific format than the event log viewer.

Deleting Events

You can permanently remove recorded events from the software's database. To do so, select the events that you want to delete. If you want to delete more than one event, hold down the <Ctrl> key while you select the events with your mouse. After you select the desired events, click on *Delete Events*. A confirmation box lets you confirm or cancel the removal of the events.

NOTE: If you remove entries from the event log database, the size of the database will not decrease until you compact the database. See "Compacting the ODBC Database."

Clearing Alarms

To mark specific alarms as cleared, select the event(s) in the Event Log Viewer and click on *Clear Alarm(s)*. To clear all alarms, select *Tools/Clear All Alarms*. A confirmation box lets you confirm or cancel the operation.

Selecting *Clear All Alarms* sets all device states to None and clears all active alarms for all devices. The icon for each device returns to the color mapped to the None state (normally green).

Resynchronizing Alarms to the Database

It is possible that through misuse of Netelligent Management Software, such as shutting down the software incorrectly, the alarm-state colors of the icons on the network maps might be incorrect. For example, a device icon may be red (or other color assigned to the "critical" state) when the actual state is not critical. To correct the icon color, select *Tools/Resync Alarms to Database*. This causes the software to completely re-load all alarms from the Event Log and re-assign the correct device states to all icons.

Setting the Maximum Number of Event Log Entries

To set the maximum number of event log entries, select *Tools/Preferences* to display the Properties dialog box. Then select the Event Log tab.

Number of Events to Keep in Event Log – enter the desired maximum number of event log entries the software can store in its event log database. When the database exceeds this number, it starts to delete older event log entries. The default value is 50000. The minimum allowable value is 500.

Number of Events to Show in Event Log Viewer – enter the desired maximum number of event log entries the software can display in the Event Log Viewer. The default value is 5000. The minimum allowable value is 10.

Chapter 3
Managing Netelligent Hubs and Switches

Compaq Netelligent Management Software provides an easy way to configure, monitor, and manage Compaq Netelligent hubs and switches using an intuitive user interface. The Compaq Netelligent Management Software displays accurate graphical representations of Netelligent products, complete with the current LED status and any installed components.

In addition to providing physical views of products, Compaq Netelligent Management Software lets you view various types of information, such as configuration settings, port statistics, and system information, by clicking the mouse pointer on control buttons or *hotspots*, which are located on the product graphics.

This chapter describes basic graphical controls, such as menu options and buttons, that are common to all Netelligent switch and hub product graphics. For information about configuring and managing a specific Netelligent hub or switch, refer to the online help for the product.

Context-Sensitive Help

Help is available for any open dialog box by taking any of the actions shown below:

- Pressing the <F1> key, or <Shift>+<F1>
- Clicking on the **Help** button on a dialog box

Operation Fundamentals

This section provides information about management functions that are common to all Compaq Netelligent switches and hubs.

Displaying a Netelligent Product Graphic

To display the graphic for the Netelligent switch or hub you want to manage, double-click on the product icon in your Main map.

A graphical representation of the product is displayed. For example, the following illustration shows a stack of Netelligent 2016 hubs. The status bar below the button bar on the device graphic displays information about the device. For example, the status for the hubs below is “OK.”

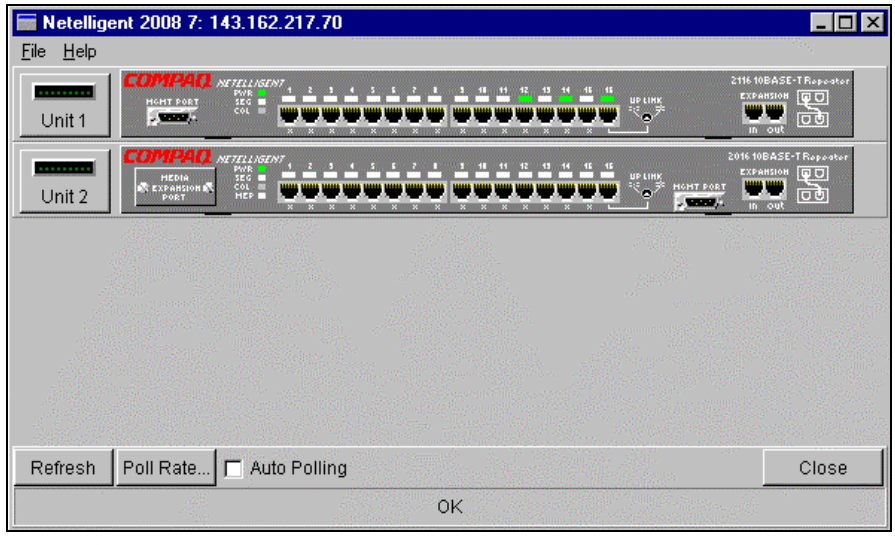


Figure 3- 1. Netelligent 2000 Hub Graphic

Using the File Menu

The File menu provides the following options that correspond to the button bar at the bottom of the screen:

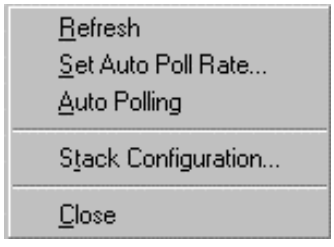


Figure 3- 2. File Menu

Refresh — Select **Refresh** to re-poll the device and update the display.

Poll Rate — Select **Set Auto Poll Rate…** to display the Poll Rate dialog box, which lets you set the auto polling rate from a minimum of 0 seconds to a maximum of 999,999 seconds. Polling devices too frequently can cause network congestion.

Auto Polling — Select **Auto Polling** to activate the auto polling function. The Compaq Netelligent Management Software automatically polls the currently selected device at the interval you specified with the Set Auto Poll Rate option.

Stack Configuration — Select **Stack Configuration** to display the Stack Config box, which lets you view various configuration settings via option buttons. See “Viewing the Stack Configuration” for details of this option.

Note: The Stack Configuration option is available for Netelligent 3000 group stackable hubs and appears as an option in the button bar. See “Using the Button Bar” in this chapter.

Using the Help Menu

Select the Help menu to display on-line help for the Compaq Netelligent Management Software.

Using the Button Bar

Each product graphic displays a button bar at the bottom of the screen. The button bar provides the same options as the File menu. See “Using the File Menu” for descriptions of these options.

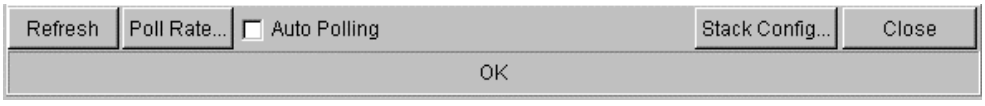


Figure 3- 3. Button Bars

Note: The Stack Config button is displayed only on Netelligent 3000 group hubs.

Refreshing the Display

Refreshing the screen re-polls the device and displays the most current information, or re-displays the product graphic after you clear the screen. To refresh the screen, select **Refresh** from the File menu or button bar.

Setting the Auto Poll Rate

You can set a specific interval at which a product or product stack is polled for the most current information. To set the poll rate, select **Set Auto Poll Rate** from the File menu or **Auto Polling** from the button bar. The following dialog box is displayed:

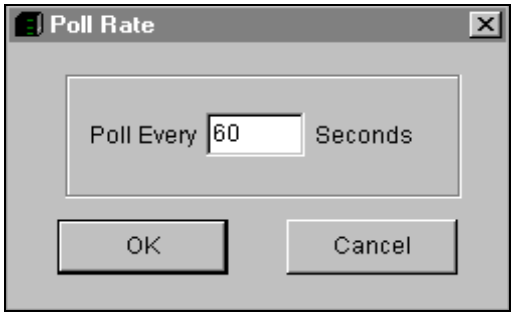


Figure 3- 4. Poll Rate Box

Enter a value from 0 seconds to 999,999 seconds and select **OK**, or select **Cancel** to close the box without setting a value. (Setting the value to 0 turns off auto polling.) Polling devices too frequently can cause network congestion.

Seconds	Minutes
60	1
600	10
900	15
1800	30
2700	45
3600	60

Enabling Auto Polling

When you enable auto polling, the software automatically polls the device at the time interval you specified in the Poll Rate box and updates the display.

To enable auto polling, select **Set Auto Poll Rate** from the File menu so that a check mark (✓) appears next to the option. Or, click on the small check box next to Auto Polling on the button bar so that an X appears. To disable auto polling, click on either location so that the check mark or X disappears.

Viewing the Stack Configuration

If the Netelligent product you are managing has one IP address per stack, such as a Netelligent 3000 group product, the Stack Configuration option is enabled in the File menu and button bar. Select this option to view the stack configuration dialog bos, which contains information about system status, the IP configuration, and traps.

Chapter 4
Using the MIB Browser

This chapter describes the MIB Browser accessed on the Compaq Netelligent Management Software main screen as described in Chapter 2.

The MIB Browser is a graphical display you can use to locate MIB variables, and, where possible, obtain the values of the variables, write to the variables, and create reports to monitor them.

This chapter contains three major sections, as follows:

- **Online Help**, a description of the online help features available to you while using the MIB Browser.
- **MIB Browser Description**, an overall physical description of the MIB Browser.

You can find important related information in the following places:

- Appendix A, “SNMP Management Concepts,” is an introduction to SNMP management and MIB structure. If SNMP management is new to you, read Appendix A before proceeding with this chapter or using Compaq Netelligent Management Software SNMP features.
- Chapter 5 describes reports that you can set up using the MIB browser.

Online Help

The MIB Browser Online Help provides the functions listed below:

- Context-sensitive help for dialog boxes
- Step-by-step help for procedures, such as creating objects
- A Help Cursor you can use to find information about menu commands

Click on any green-colored message to find more help about that topic.

If the Help Selector you see does not match the one shown above, click on the **Help** button to find more information about the choices you have.

Context-Sensitive Help

Help is available for any MIB Browser open dialog box by taking any of the actions shown below:

- Pressing the <F1> key, or <Shift>+<F1>
- Clicking on the **Help** button on a dialog box
- Selecting **Help for this Window** from the Help menu

MIB Browser Description

Select the icon of any SNMP-manageable object on the Compaq Netelligent Management Software main screen, then select the MIB Browser button in the button bar. (Or, select **Edit/SNMP Statistics/MIB Browser** in the menu bar, or right-click on the device icon and select **SNMP Statistics/MIB Browser** from the menu.)

If the object you selected does not have a pop-up menu, it is not SNMP-manageable and therefore you cannot use the Browser with that object.

Main Window

When you start the MIB Browser, *mib-2* is the default MIB that is displayed. It is similar to the one shown in Figure 4-1.

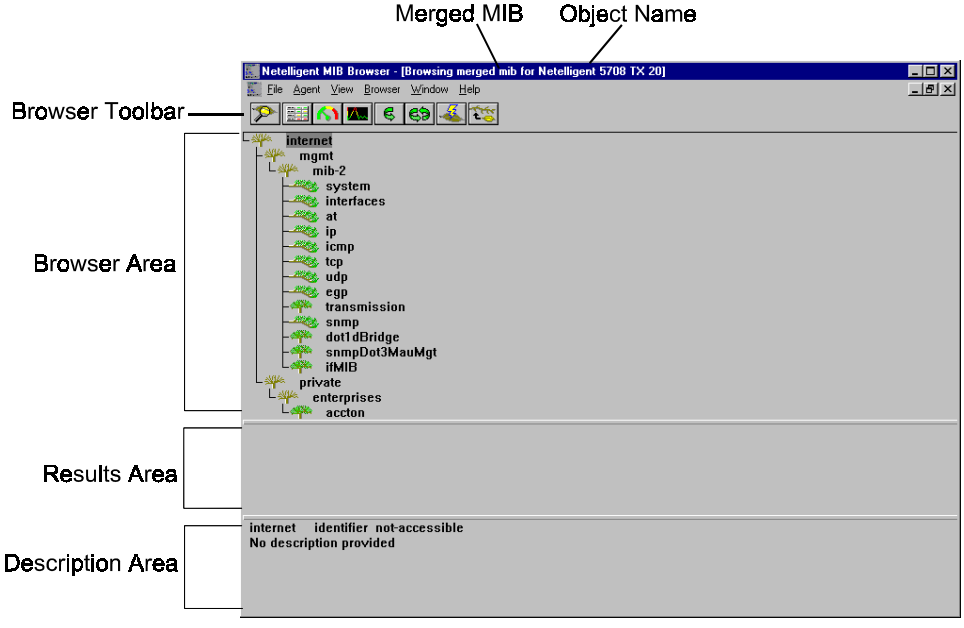


Figure 4-1. MIB Browser Top Screen

The MIB Browser displays a graphical view of the MIBs you selected under Supported MIBs. This is a merged list of all MIBs (earlier versions of Compaq Netelligent Management Software listed MIBs separately). Its tools let you get and set MIB variable values, and create reports.

The MIB Browser can be divided into the areas listed below. You can find more information about each area later in this chapter.

- **Title Bar:** Displays the name of the merged MIB and the SNMP-manageable object

- **Browser Toolbar:** Has tools that perform the following functions: Get Selected, Create Table, Create Dial, Create Graph, Get Next, Get All Next, Set, and Clear Selections.
- **Browser Area:** Shows the structure of the merged MIB in tree format
- **Results Area:** Shows the results of actions taken with the Browser toolbar or with the menu. A vertical scroll bar is included to display multiple lines of Result Area data.
- **Description Area:** Shows additional information (such as the variable name, type and additional descriptive information) about a selected MIB item. Movable bars on the top and bottom of the Description area allow it to be resized at any time.

The Browser's Graphical Representation

The Browser area of the MIB Browser represents the structure of the MIB as a tree diagram. Figures 4-2 and 4-3 illustrate the correspondence between the MIB structure and the Browser's graphical representation:

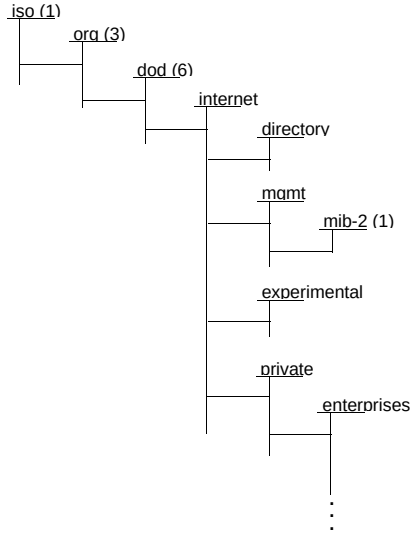


Figure 4-2. Diagrammatic representation of MIB structure

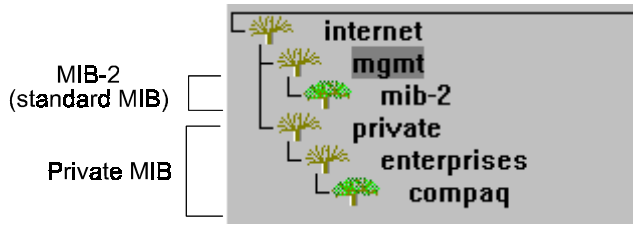


Figure 4-3. MIBs as represented by the MIB Browser

Figure 4-3 shows a diagrammatic representation of a collapsed MIB structure. This structure shows both RFC1213 (the standard *mib-2*) and the top-level container for Compaq enterprise specific MIBs. Figure 4-3 shows how the Browser displays both MIBs in collapsed form.

In fact, every MIB initially is displayed in the Browser as a collapsed tree diagram that begins with the "internet" subtree (object identifier 1.3.6.1).

Every private MIB initially is displayed similar to the Compaq enterprise specific MIB, shown in Figure 4-3; the IAB-assigned vendor name is displayed under the "enterprises" subtree (this term is defined in the next section).

Browser Representation of an Expanded MIB

This section explains how the Browser represents the MIB's hierarchical container structure. The highest-level container is the *subtree*. It is represented by one of the symbols shown in Figure 4-4:

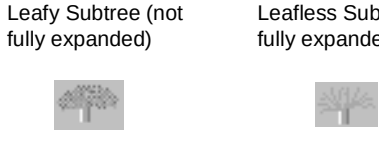


Figure 4-4. The Subtree

Every subtree, by definition, contains lower-level subtrees and/or branches. The presence of leaves on the branches of the subtree indicates that the subtree has not been fully expanded. To expand a leafy subtree, double-click on it.

The next-lower level, the *branch*, is represented by one of the symbols shown in Figure 4-5:

Figure 4-5. The Branch

The branch is a logical container, since it contains items that are related to each other. Every branch, by definition, contains lower-level branches, twigs and/or leaves. (Some branches do not contain any twigs.) The presence of leaves on the branch indicates the branch has not been fully expanded. To expand a leafy branch, double-click on it.

A *broken branch* is a branch for which there are no lower-level entities (no lower-level branches, no twigs, no leaves, and no traps). A broken branch represents a level of MIB structure that was planned, but not implemented. An example is the "transmission" branch of RFC1213.

The next-lower level of structure, the *twig*, is represented by one of the symbols shown in Figure 4-6:

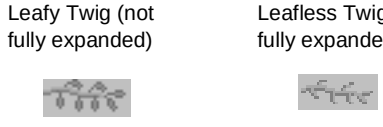


Figure 4-6. The Twig

A twig represents a set of MIB table variables. A table is a type of report and is discussed in more detail in Chapter 5. To expand a leafy twig, double-click on it.

The lowest levels of structure, the *leaf* and the *trap*, are represented by the symbols shown in Figure 4-7:

Figure 4-7. Leaves and Traps

Initially, the leaf is displayed green in color; when you click on it to select it, its color changes to yellow.

A trap represents a *trap variable*. Trap variables are not configurable using the MIB Browser. They contain read-only information. More information about traps can be found in Appendix A.

Object Text Colors

In addition to the graphical representation of the organization of the MIB, the color of the MIB variable text gives you information about what type of variable it is. Table 4-1 below explains the meanings of text colors:

Table 4-1
MIB Browser Text Color Meanings

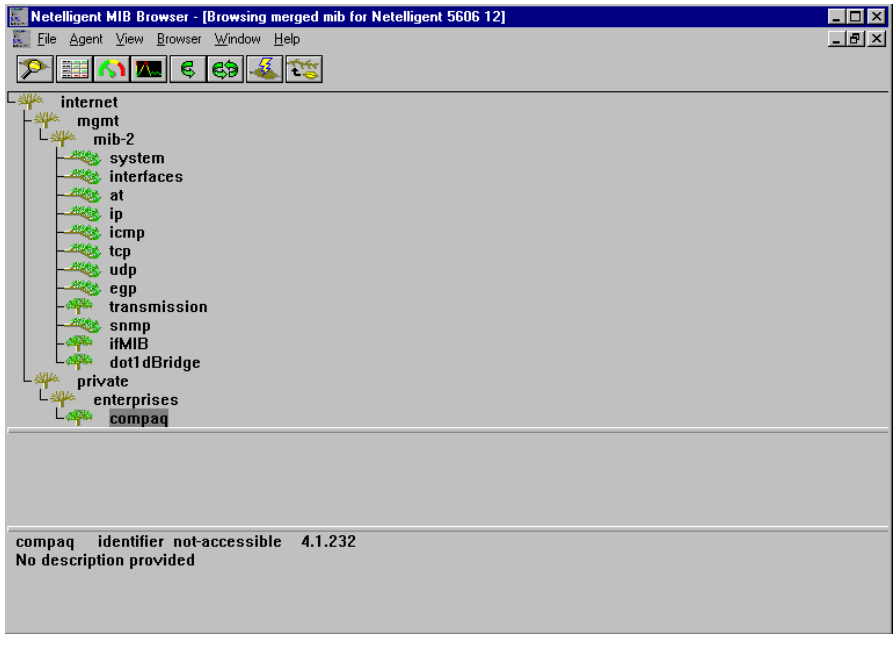
Object Type and Symbol	Text Color	Meaning
Subtree	Black	Not-accessible; variable values cannot be obtained (Get or Set commands are not valid).
Branch	Black	Not-accessible; same as for subtree.
Broken Branch	Black	Not-accessible; represents a branch for which there are no lower-level entities (branches, twigs, traps or leaves); expansion was intended, but not carried out.
Twig	Blue	A set of table variables. Can Get, can Set (with sufficient rights to the agent).
Trap	Red	Trap variable; see Chapter 6.
Leaf	Green	Read-only variable; can Get, cannot Set.
	Blue	Read-write variable; can Get, can Set (with sufficient rights to the agent).
	Yellow	Selected variable.

Hands-On Examples of the MIB Structure

This section walks you through the Browser's graphical representation of a MIB structure. For example purposes, this chapter uses RFC1213.CMB, the compiled version of *mib-2*, a standard MIB. RFC1213.CMB and Compaq MIBs to support Netelligent devices are shipped with Compaq Netelligent Management Software. They are stored in the *MIBS* directory in the directory where you installed Compaq Netelligent Management Software.

Preparing for Hands-On Examples

To begin the MIB Browser, from the main menu bar, double-click the MIB Browser icon. Or, right click on the icon of any SNMP-manageable object. This displays a pop-up menu. From the pop-up menu, select **SNMP Statistics**, **MIB Browser**. The object's MIB Browser appears similar to the following figure:



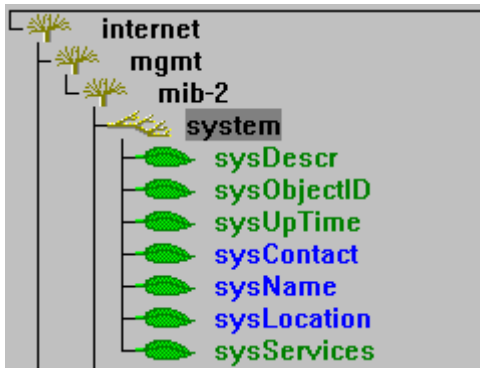
If *mib-2* does not appear in the MIB field in the previous figure, with a simple two-step procedure you can add it to the list. See the subsection “Adding and Deleting Currently Compiled MIBs” under the section “ Selecting a MIB to Manage the Agent” in this chapter.

Examples of Subtrees and Branches

The previous figure contains three subtrees, called *internet*, *mgmt*, and *mib-2*. The *mib-2* subtree is already expanded and contains 10 leafy branches and one broken branch (called *transmission*).

Examples of Branches and Leaves

1. Double-click on the *system* branch, which expands it as shown in the following figure:

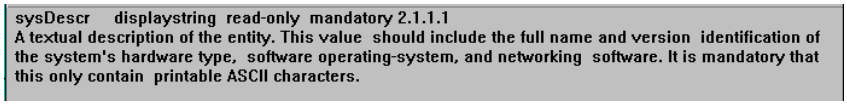


The *system* branch contains seven leaves, called *sysDescr*, sysObjectID, *sysUpTime*, *sysContact*, *sysName*, *sysLocation*, and *sysServices*. The variable group name for these leaf objects is *sys*.

Of these leaves, four (*sysDescr*, *sysObjectID*, *sysUpTime*, and *sysServices*) have green text, meaning the variables are read-only; the other three (*sysContact*, *sysName*, and *sysLocation*) have blue text, meaning they are read-write.

Finally, notice that the word "system" is black, indicating the branch itself is not-accessible; this is confirmed by the text in the Description area.

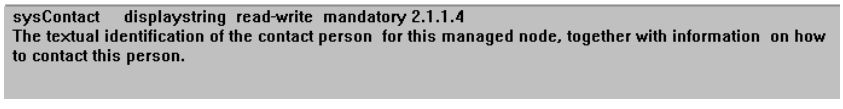
2. Click on the *sysDescr* leaf, which causes the color of the leaf to change to yellow and displays a description of the *sysDescr* variable in the Description area of the MIB Browser, as shown in the following figure.


sysDescr displaystring read-only mandatory 2.1.1.1
A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.

The partial object ID for *sysDescr* (2.1.1.1) is displayed. The full object identifier (beginning with the *iso* subtree) for *sysDescr* is 1.3.6.1.2.1.1.1.

The descriptive text confirms the fact that *sysDescr* is a read-only variable and also provides information about the *sysDescr* variable.

3. Use the arrow keys to move to the *sysContact* leaf, which displays the text shown below:

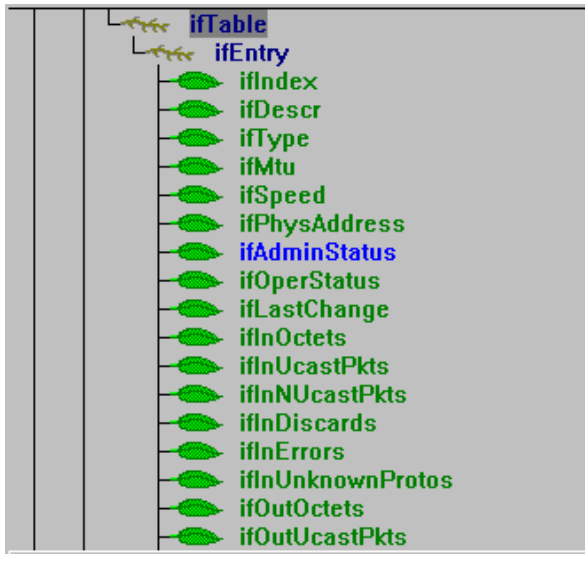

sysContact displaystring read-write mandatory 2.1.1.4
The textual identification of the contact person for this managed node, together with information on how to contact this person.

Notice that the *sysDescr* is yellow, indicating it has been selected, while the *sysContact* leaf is still green. Using the arrow keys lets you view the descriptions of MIB objects without selecting them.

Examples of Twigs and Resolving Indices

1. Double-click on the *interfaces* branch, which expands to reveal one leaf (*ifNumber*) and one twig (*ifTable*). The *ifNumber* text is green, meaning it is read-only. The *ifTable* level is a twig, which means the lower-level objects it contains belong in a table.

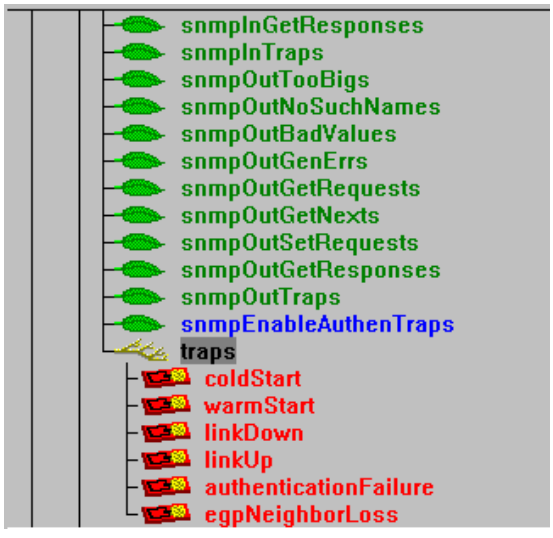
2. Double-click on the *ifTable* twig, which expands it as shown in the following figure:



The *ifEntry* twig contains entries for the *ifTable*, which can be displayed together in a table report.

Example Trap

Double-click on the *snmp* branch, then double-click on the *traps* branch, which expands as shown in the following figure:



The *traps* branch contains trap variables (*coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss*). The text beside each trap variable is red.

You can click on each trap to obtain information about it, but double-clicking on a trap results in a red-colored message in the Results area. More information about traps can be found in Appendix A.

Using MIB Browser Tools and Menus

This section explains how to use the Browser toolbar, and how to use the pop-up menu and the Browser menu to execute SNMP commands.

Figure 4-8 shows Browser menu and tools:

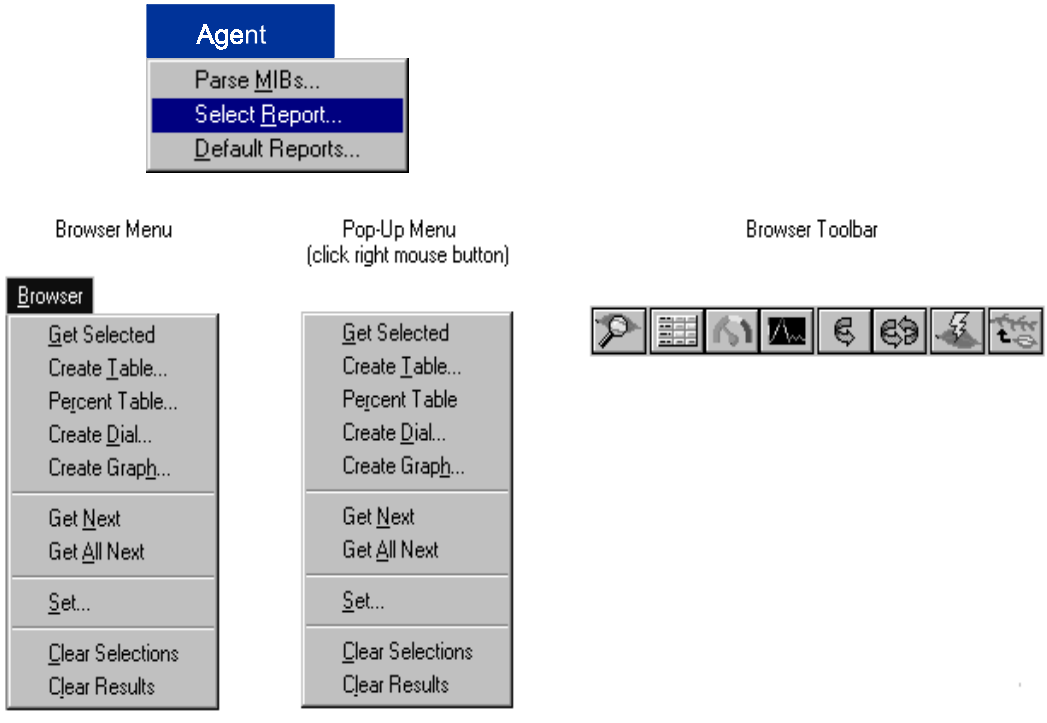
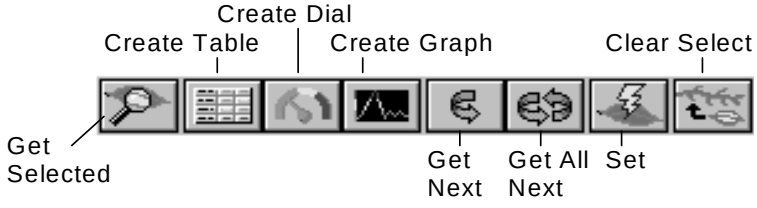


Figure 4-8. MIB Browser Tool Sets

Using the Browser Toolbar

The Browser toolbar performs various functions with the click of your mouse. The following figure shows a labeled toolbar (the name of each tool is displayed while you hold down the left mouse button):



SNMP Command Summary

Table 4-5 summarizes the meanings of SNMP commands implemented by the Browser tools. For more information, see "SNMP Commands" in Appendix A, "SNMP Management Concepts."

Table 4-2
SNMP Command Summary

Command Name	Meaning
Get Selected	Obtain current variable value. Valid for any read-only or read-write variable.
Set	Write new value for variable; valid for read-write variables (displayed in blue text in the Browser). Your ability to successfully complete a Set command depends on the rights the community has to the agent.
Get Next	Obtain the value of the next variable after the currently selected variable.
Get All Next	Obtain the current value of the selected variable and all subsequent variables in order until you stop the process.

Hands-On Examples of Using Tools and Menus

This section shows you how to use the Browser toolbar, the MIB Browser pop-up menu, and the Browser menu. The examples shown all use RFC1213.CMB, the compiled version of RFC1213 (*mib-2*). The examples in this section apply to both the Browser toolbar and the menu, since they function identically.

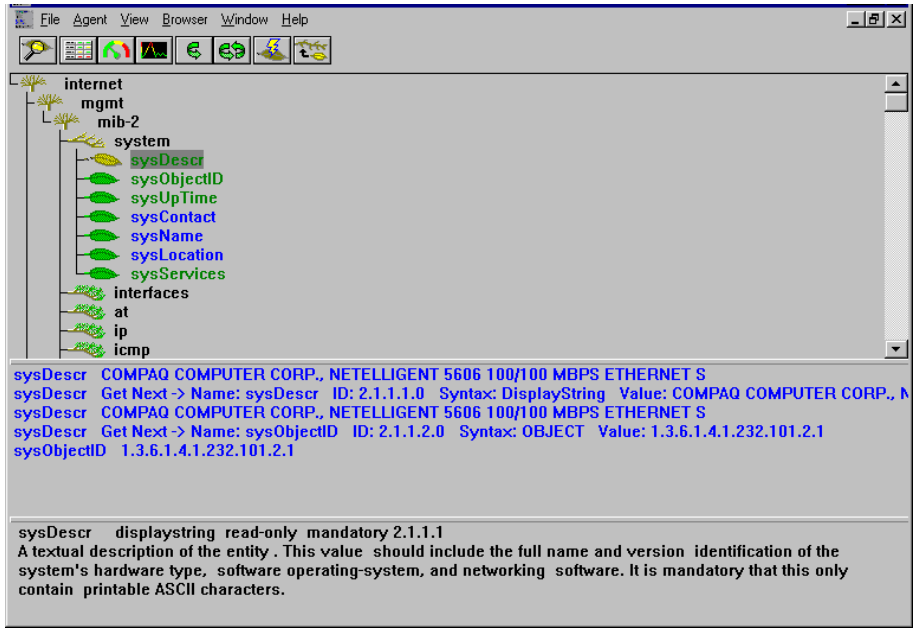
Preparing for Hands-On Examples

To begin, open the MIB Browser for any SNMP-manageable object that has *mib-2* selected. To do so, click on the icon of any SNMP-manageable object. This displays a pop-up menu; from the menu, select **SNMP Statistics, MIB Browser**.

Using the Get Selected, Get Next, and Get All Next Tools

To get a current variable value (G*et Selected*), get the current value of the selected variable and the next variable (*Get Next*), or get the current value of the selected variable and the next variable (*Get All Next*), perform these steps:

1. Double-click on the *system* branch, if it is not already expanded.
2. Click on the *sysDescr* leaf and click on the **Get Selected** tool (or select **Get Selected** from the menu). The Results area displays the value of the *sysDescr* variable.
3. Click on the **Get Next** tool twice (or select **Get Next** twice from the menu). The first time you use the **Get Next** tool, it displays the current value of the selected variable. All subsequent selections of the **Get Next** tool displays the current value of the *next* variable in the MIB tree. The Results area then displays five lines. The first *sysDescr* line is left over from the previous Get command.


File Agent View Browser Window Help
internet
mgmt
mib-2
system
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
interfaces
at
ip
icmp
sysDescr COMPAQ COMPUTER CORP., NETELLIGENT 5606 100/100 MBPS ETHERNET S
sysDescr Get Next -> Name: sysDescr ID: 2.1.1.1.0 Syntax: DisplayString Value: COMPAQ COMPUTER CORP., N
sysDescr COMPAQ COMPUTER CORP., NETELLIGENT 5606 100/100 MBPS ETHERNET S
sysDescr Get Next -> Name: sysObjectID ID: 2.1.1.2.0 Syntax: OBJECT Value: 1.3.6.1.4.1.232.101.2.1
sysObjectID 1.3.6.1.4.1.232.101.2.1
sysDescr displaystring read-only mandatory 2.1.1.1
A textual description of the entity . This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.

4. Click on the **Get All Next** tool (or select **Get All Next** from the menu). The Results area then begins scrolling through the values of all variables, beginning with *sysDescr*. Take one of the actions below to pause scrolling or stop the Get All Next command:

   - **To Pause scrolling**: Click on the **Get All Next** tool (or select **Get All Next** from the menu); scrolling resumes when you click the tool again. The last variable to be displayed before you paused is redisplayed when scrolling resumes.

   - **To Stop the Get All Next command**: Either click on the **Clear Selections** tool, or select **Clear Selections** from the menu, or press the <**C**> key.

5. Select **Clear Results** from the Browser menu. Click the **Clear Select** tool, or select **Clear Selections** from the menu.

6. Click on the *sysDescr* leaf in the system branch.

7. Double-click on the *icmp* branch of the Browser, which expands the branch. Then click on the *icmpInTimeEscds* leaf and click on the **Get Selected** tool (or select **Get Selected** from the menu). The values of both selected variables (*sysDescr* leaf on the system branch and the *icmpInTimeEscds* leaf on the *icmp* branch) are displayed in the Results area.
8. Click on the **Get All Next** tool (or select **Get All Next** from the menu). This results in a red-colored message in the Description area. That is because you cannot execute a Get All Next command with more than one leaf object selected.
9. Click the **Clear Selections** tool (or select **Clear Selections** from the menu) to remove all previously-selected leaf objects, then select **Clear Results** from the menu to clear the Results area.

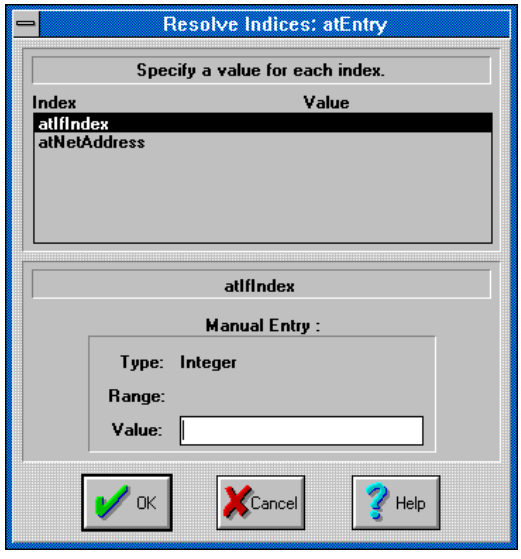
Using the Set Command Tool

Your ability to successfully complete a Set command depends on the rights the community has to the agent. To write a new value for variable (Set), follow these steps:

CAUTION: Using the Set command changes values of variables at the agent. Before using the command, make sure the variable you plan to change will not adversely affect the operation of the agent.

1. Double-click on the *icmp* branch of the *mib-2* subtree, if it is not already expanded.
2. Click the *icmpInTimeEscds* leaf, then click the **Set** tool (or select **Set** from the menu). A red-colored message is displayed in the Description area; this is because the *icmpInTimeEscds* variable is read-only. This is indicated by its green text, and also by its description the Description area of the Browser. The Set command is not valid for read-only variables.
3. Double-click on the *icmp* branch to collapse it.
4. Double-click on the *at* branch, which expands it to reveal the *atTable* twig. Then double-click on the *atTable* twig to expand it.

   The *atTable* twig expands to reveal another leafless twig (*atEntry*). The leafless *atEntry* twig contains three leaves (*atIfIndex*, *atPhysAddress*, and *atNetAddress*). Each leaf in the twig represents at least one row in the *atEntry* table. Notice that the text beside each leaf is blue, indicating each leaf is read-write.
5. Click on the **Clear Selections** tool (or select **Clear Selections** from the menu).
6. Click on the *atIfIndex* leaf, then click on the **Set** tool (or select **Set** from the menu). The Resolve Indices dialog box is displayed as shown in the following figure:



To complete the Set command for this variable, you must provide values for two different indices, *atIfIndex* and *atNetAddress*.

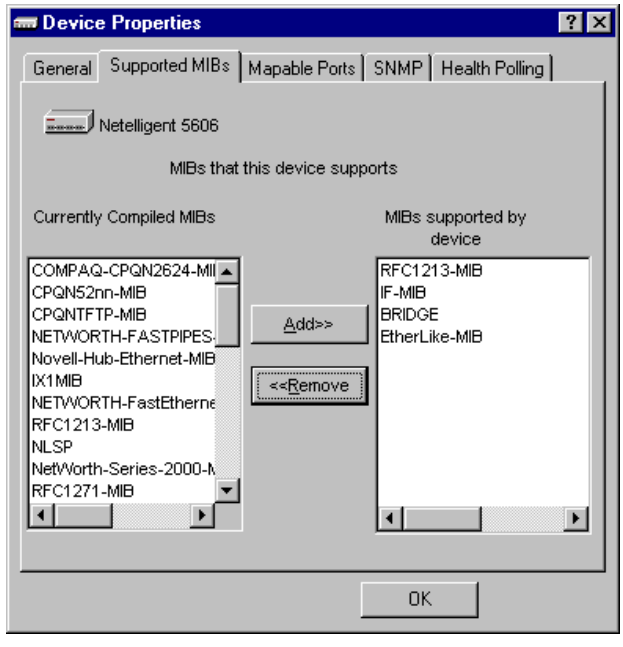
To see values of the indices for any particular set of table variables (leaves contained by a twig), you can create a table report. To do so, click on the twig, which selects all the leaves it contains. Then use the Table tool, or select **Create Table** from the menu. You can find more about creating reports in Chapter 5.

Selecting a MIB to Manage the Agent

You can manage an SNMP agent with a MIB. Selecting one or more loaded MIBs lets you use those MIBs to manage the agent. A MIB can manage more than one agent.

Before you add any MIBs, check to see which ones are already loaded by performing these steps:

1. Right-click the icon of any SNMP-manageable object on the Main Map.
2. From the pop-up menu, select **Properties**. The Supported MIBs tab of the Device Properties dialog lists "MIBs supported by this device."



NOTE: When you drag a device from the Network Devices window, place it on the Main Map, and assign it an IP address, the supported MIBs for that device automatically appear in the "MIBs supported by this device" listbox.

Adding and Removing Currently Compiled MIBs

To add currently compiled MIBs (including RFC.1213 for *mib-2*, if it is not currently listed) to those currently in the device, follow these steps:

1. Select the MIB you want to add from the Currently Compiled MIBs listbox.
2. Click Add. The MIB moves to the MIBs supported by this device listbox.

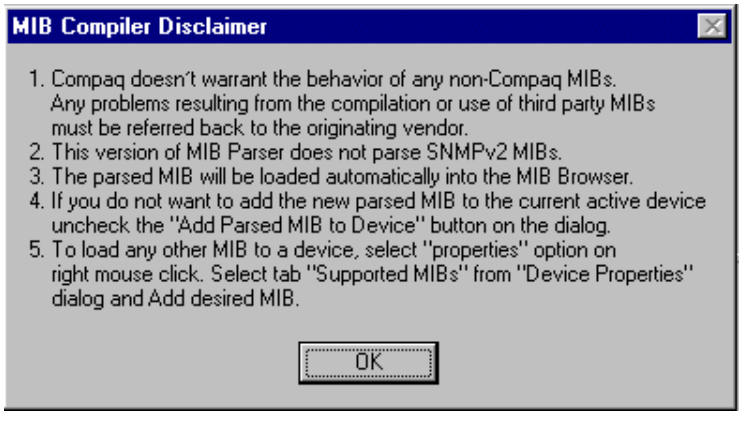
To remove a currently compiled MIB, follow these steps:

1. Select the MIB you want to delete from the MIBs supported by this device listbox.
2. Click **Remove**. The name of the MIB disappears from the MIBs supported by this device listbox.

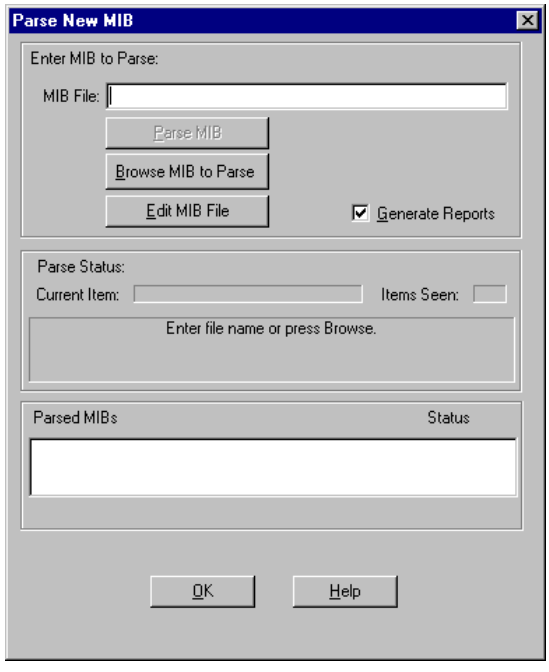
Parsing a MIB

If you want to add a MIB that is not currently compiled, follow these steps:

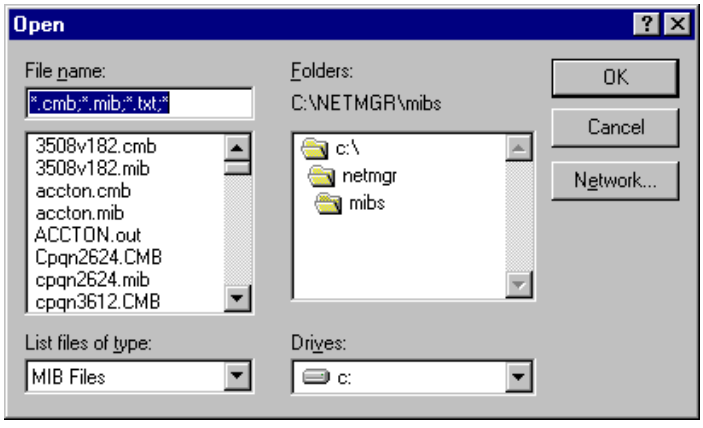
1. Start the MIB Browser by clicking any SNMP-manageable object on the Main Map and selecting the MIB Browser icon from the Compaq Netelligent Management Software Main window.
2. Select **Parse MIBs** from the **Agent** menu. The following message appears:


MIB Compiler Disclaimer
1. Compaq doesn't warrant the behavior of any non-Compaq MIBs. Any problems resulting from the compilation or use of third party MIBs must be referred back to the originating vendor.
2. This version of MIB Parser does not parse SNMPv2 MIBs.
3. The parsed MIB will be loaded automatically into the MIB Browser.
4. If you do not want to add the new parsed MIB to the current active device uncheck the "Add Parsed MIB to Device" button on the dialog.
5. To load any other MIB to a device, select "properties" option on right mouse click. Select tab "Supported MIBs" from "Device Properties" dialog and Add desired MIB.
OK

4. Press **OK** to continue. Then Parse New MIB dialog appears:



5. Click on **Browse MIB to Parse** to locate a MIB. This reveals the dialog box shown in the following figure:



Select a MIB file to load from the list in the left listbox. The MIBs shipped with the Compaq Netelligent Management Software are all in the *mibs* directory, as shown above.

6. If you want to load your own MIB, you can use this dialog box to locate it. The Compaq Netelligent Management Software compiles it for you.

   IMPORTANT: You cannot load a MIB that was compiled by another program. You must let the Compaq Netelligent Management Software compile the MIB for you.

7. Click **OK** to return to the Parse New MIB dialog box after you load a new MIB. Compaq Netelligent Management Software parses the MIB and automatically adds the parsed MIB to the list of selected MIBs in the selection box.

8. If you prefer not to add the parsed MIB to the list, be sure you uncheck the **Add Parsed MIB to Current Device** box before browsing the MIB to parse.

9. When you are done, click on **OK** repeatedly until you return to your starting point.

Chapter 5
Using MIB Browser Reports

This chapter describes the various types of reports you can set up using the MIB Browser, which is described in Chapter 4.

Creating Reports

Reports and traps are two sets of tools you can use to monitor an SNMP agent. *Reports* display data in real-time, and are ideally suited for baselining the network, determining reasonable thresholds, or for closely monitoring an emerging trouble spot. There are four types of reports you can create: tables, dials, graphs and percent tables. Since reports consume resources on your machine whenever they are open, and since updating report data causes traffic on the network, you should not use reports for long-term monitoring.

Another way to receive fault information about your network is through the use of traps. *Traps* are defined in the agent's MIB and send messages to the management console immediately after the occurrence of the condition that triggered them. Traps do not require constant polling, generate no traffic on the network until a message is actually sent, and require no resources on your machine. For those reasons, traps are recommended for long-term monitoring. See Chapter 6, “Handling Traps” for further information.

MIB Variable Type and Syntax

For SNMP-manageable objects, the type and syntax of the MIB variable you select must match the type of report you want to create, as shown below.

- **Table reports:** Any MIB variable displayed as a leaf can be included in a table (except for write-only variables). Leaves contained in a twig are best suited for tables. Each variable is displayed as a row in a table report. Table reports display the total count of all variables since the agent's (or the report's) counters were started or reset.

- **Dial and Graph reports:** Restricted to variables with counter or gauge syntax. Each variable is displayed in a separate report window for dial or graph reports. Dial and graph reports track average variable counter values over time. The difference between dial and graph reports is that graph reports display historical data, while a dial displays a "snapshot" of the high, average, and current counter values.

You can select one or more variables to display in a report. The variables you select do not have to belong to the same branch or the same subtree, but you do have to remember that if you select a table variable from a particular twig, all other variables must be contained in the same twig.

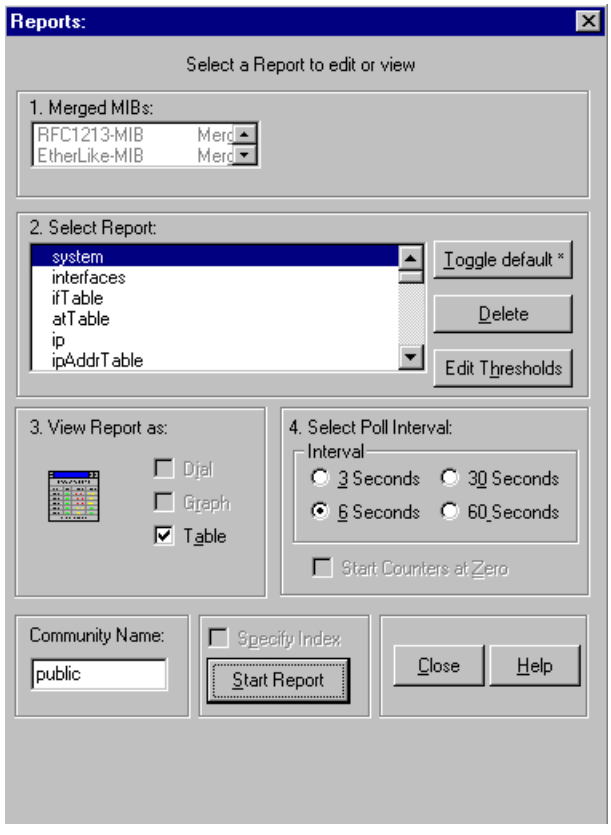
Two Classes of Reports

This section discusses two classes of reports. *Existing* reports are reports that have been previously defined, either by you or by using new variables made available by compiling a MIB. You can launch any existing report by selecting the report from the Reports dialog box. This is covered in the next section.

Custom reports are reports that you create by selecting MIB variables from the MIB Browser. Subject to the rules stated in the section "MIB Variable Type and Syntax" above, you can select virtually any combination of variables to display on a report. Examples of custom reports are found in the section "Defining Custom Reports" later in this chapter.

Starting an Existing Report

Choose *Agent/Select Report* from the menu bar. The Reports dialog box appears, similar to the one shown below:



All existing reports for the selected MIB are displayed in the Select Report selection box. Click on the report you wish to start and click the *Start Report* button. Other related fields and buttons on this dialog box are described below:

- **Merged MIBs:** (Read Only) Lists all the merged MIBs

- **Select Report:** Listbox containing MIB variables you can use to generate reports. Creates any reports for all the tables in the merged MIBs. These reports are created (but not started) for MIB branches and twigs that contain leaves. In the Reports dialog illustration shown above, all reports displayed in the Select Report selection box were created by selecting **Agent, Select Report** from main pull-down menu. You can use the Reports dialog box to start any one of these reports at a time.
- **3. View Report as check boxes:** Allows you to select the view options for the report (dial, graph, or table). Depending on the syntax of the variables included in the report, some of these options may be grayed-out.
- **4. Select Poll Interval check boxes:** Select the length of time the Console waits before polling the agent to update report data. The four options are: 3, 6, 30, and 60 seconds. The shorter the interval you select, the more often the report display is updated; however, a shorter interval also causes more traffic on the network, so a short interval is not recommended on a busy network.
- **Community Name text field:** Enter a valid community name for the agent. Community names are case-sensitive.
- **Specify Index check box:** Select an index of a single or multi-index report. This check box is grayed-out for tables that are not indexed. If this box is unchecked, the following scenarios can occur:
  - If the table is indexed on a single-integer index or indices, a report is generated for all rows of that table.
  - If the table is indexed on a non-integer index, you must enter values for each index.

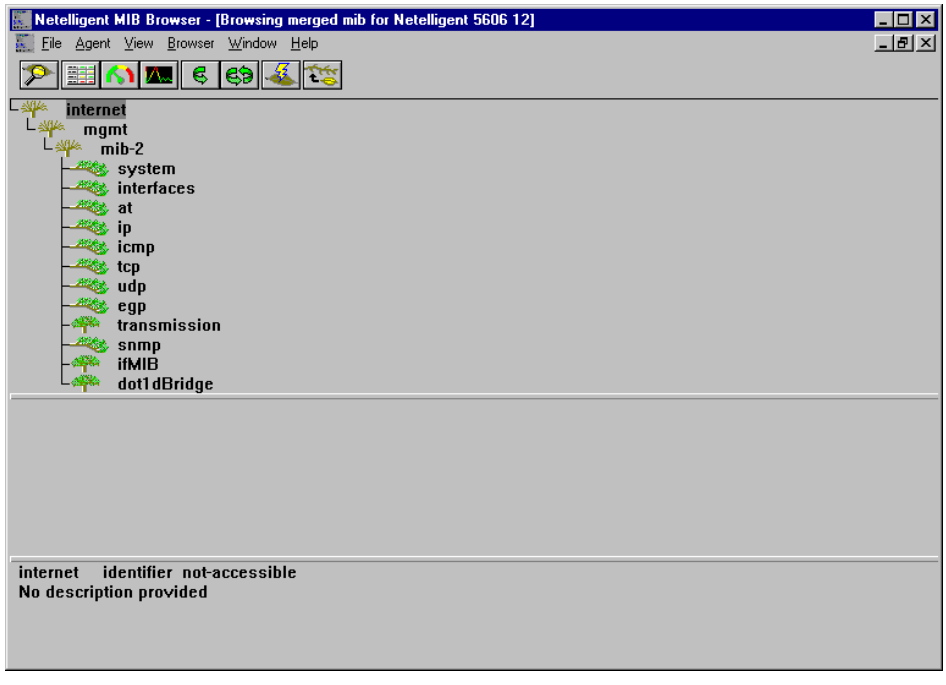
NOTE: When you generate reports by selecting one or more variables in a table, you must also select the index/indices variables in the table to view a meaningful report.

Defining Custom Reports

This section has examples of creating custom table, graph and percent table reports. The examples shown all use RFC1213.CMB, the compiled version of MIB-2. The custom reports you create are then associated with the selected object, so the same set of custom reports are available for this object later.

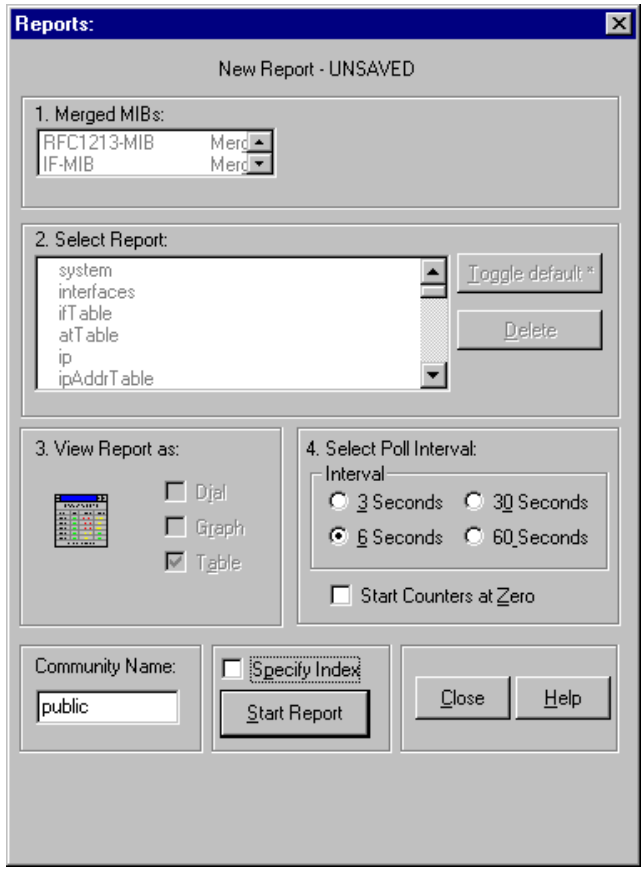
Preparing for the Examples

To begin, open the MIB Browser for any SNMP-manageable object that has RFC1213 (MIB-2) selected. To do so, select the icon of any SNMP-manageable object on the Compaq Netelligent Management Software main screen, then select the MIB Browser button in the button bar. (Or, select **Edit/SNMP Statistics/MIB Browser** in the menu bar, or right-click on the device icon and select **SNMP Statistics/MIB Browser** from the menu.)



Creating a Sample Report: Table

1. Double-click on the *interfaces* branch to expand it, then double-click on the *ifTable* twig to expand it. The *ifTable* twig has several leaves under it. You can increase the size of the Browser window by clicking and dragging one of its edges.
2. Click on the leafless *ifEntry* twig, which selects all the leaves contained in the twig. Then click on the **Table** tool (or select **Create Table** from the Browser menu). A dialog box similar to the following is displayed:



Notice that the “View Report as” checkbox has “Table” checked.

3. To create a report showing all indices for this object, click on **Start Report**. The report then appears similar to the following figure:

if Table Report for 3rd Floor Router, 6s

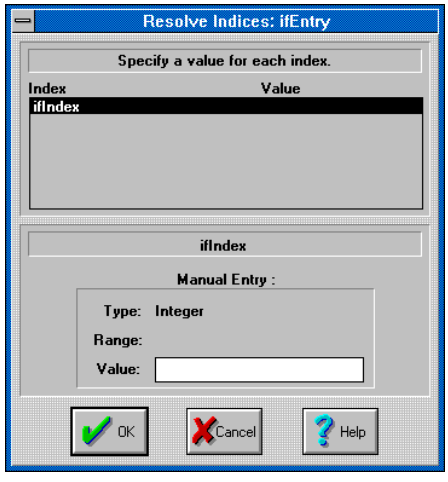
if for 3rd Floor Router				
Index	1	2	3	4
Descr	Fddi0/0	Ethernet1/0	Ethernet1/1	Ethernet1/2
Type	fddi	ethernet-csmacd	ethernet-csmacd	ethernet-cs
Mtu	4,470	1,500	1,500	1,500
Speed	100,000,000	10,000,000	10,000,000	10,000,000
PhysAddress	00-00-0C-39-06-5C	00-00-0C-39-06-64	00-00-0C-39-06-65	00-00-0C-3
AdminStatus	up	up	up	up
OperStatus	up	up	up	up
LastChange	34 days, 8 hours	32 seconds	32 seconds	32 seconds
InOctets	9,134,238	469,350	160,284	631,916
InUcastPkts	17,500	4	1,856	3,363
InNUcastPkts	406	917	2	14
InDiscards	0	0	0	0
InErrors	0	0	0	0
InUnknownProtos	0	0	0	0
OutOctets	11,793,959	19,036	2,904,446	1,436,280
OutUcastPkts	17,697	3	3,060	3,113
Updated Tue Jul 16 at 11:03:58 AM				

Notice that the first row in the table specifies the indices. Each row in the table corresponds to a MIB variable contained by the *ifEntry* twig. You can find more about report displays, including thresholds, later in this chapter.

4. To create a report for a selected index for this object, fill in the dialog box, making sure to click on **Specify Index**.

5. Then click the **Start Report** button. The Resolve Indices dialog box is displayed, as shown in the following figure.

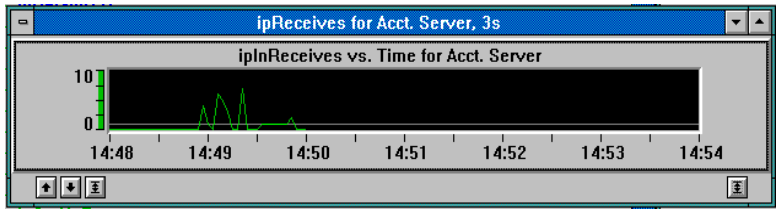
6. Enter an integer in the Value field for the index.



After entering an index, a table report is displayed showing data for *index 2*. You can find more information about report displays, including thresholds, later in this chapter.

Creating a Sample Report: Graph

1. Double-click on the *ip* branch to expand it.
2. Click on any counter or gauge variable, such as the *ipInReceives* leaf.
3. Then click on the **Graph** tool (or select **Create Graph** from the menus). A Reports dialog box is displayed similar to the one shown in the section "Preparing for the Examples." In this case, notice that the "View Report as" checkbox has "Graph" checked.
4. Then click on **Start Report**. The report is displayed similar to the following:



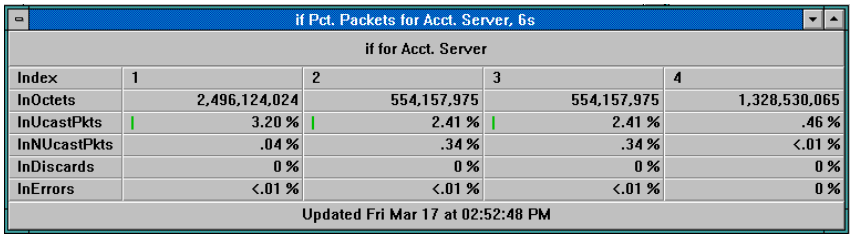
You can find more about the report display, including thresholds, later in this chapter.

Percent Table Reports

A percent table is a special type of table report that, in addition to displaying raw data, also displays each table entry as a percentage of a total number. (The last variable you select is used as the total.) Select variables that are counter or gauge syntax (since you can then set thresholds to monitor those variables), and select related variables, such as those in the same branch or twig. You can find more about setting thresholds later in this chapter.

Creating a Sample Percent Table Report

1. Open the MIB Browser for any SNMP-manageable object that has RFC1213 (MIB-2) selected for it.
2. Double-click on the *interfaces* branch to expand it, then double-click on the *ifTable* twig to expand it, as shown in the figure below:
3. Click on the following leaves, in the order shown: *ifIndex*, *ifInErrors*, *ifInDiscards*, *ifInNUcastPkts*, *ifInUcastPkts*, and *ifInOctets*.
4. Select *Percent Table* from the menus. The Reports dialog box then displays, as shown in the two previous examples. Then click on **Start Report**. The report displays similar to the one shown in the following figure:

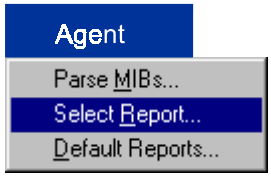

if Pct. Packets for Acct. Server, 6s
if for Acct. Server
Index 1 2 3 4
InOctets 2,496,124,024 554,157,975 554,157,975 1,328,530,065
InUcastPkts 3.20 % 2.41 % 2.41 % .46 %
InNUcastPkts .04 % .34 % .34 % <.01 %
InDiscards 0 % 0 % 0 % 0 %
InErrors <.01 % <.01 % <.01 % 0 %
Updated Fri Mar 17 at 02:52:48 PM

This report shows the percentage of various packet types relative to total packets (*InOctets*).

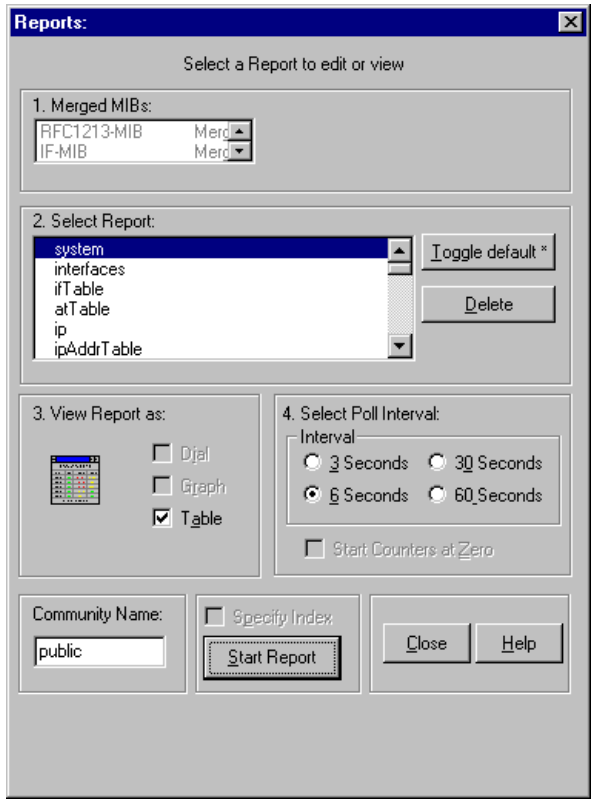
Designating Default Reports

This section explains how to designate one or more reports as *default reports*. The default reports you designate are then associated with the selected device, so the same set of default reports are available for this object later.

1. Select **Agent/Select Report** from the menu bar.



The Reports dialog is displayed:



Notice that the Report description now reads “Select a Report to edit or view” and that the Select Reports option is now available.

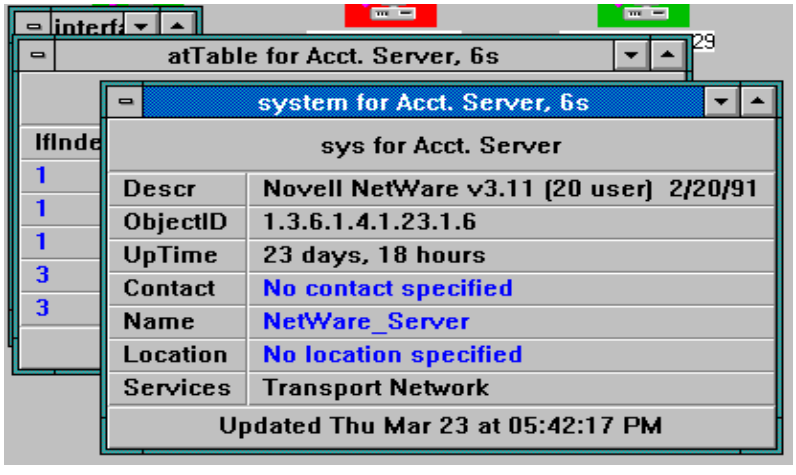
2. The Select Report selection box displays all existing reports for the MIB. Click on a report you want to designate as a default report.

3. Make any desired adjustments to report parameters. For more information about the Reports dialog box, see the section "Starting an Existing Report" earlier in this chapter or click on the Help button to access the online help.

4. Click the **Toggle default** button. An asterisk (*) then appears beside the report you selected, indicating it is now a default report, which starts whenever you select **Agent/Default Reports**.

5. Again click the **Toggle default** button. The asterisk disappears, indicating the selected report is no longer a default report.
6. Click on other reports you wish to designate as default.
7. Click on **Close** to close the dialog box.
8. Then click on the **Agent/Default Reports** menu bar.

The default reports you selected are then started. If you selected the default reports for, *interfaces* and *atTable*, the reports display similar to the following:



Deleting a Report

Deleting a report for an SNMP-manageable object removes that report not only from that object, but for all objects managed by the same MIB. Renaming the report allows it to be used for all objects managed by the MIB with the new name. Take the following actions:

1. Choose **Agent/Select Report** from the menu bar. The Reports dialog box appears.

2. The Select Report selection box contains all reports defined for the MIB that is selected in the Select MIB selection box. Click on the report you wish to delete.
3. When you locate the report you wish to delete, click on the **Delete** button.

Working With Reports

Viewing a Report as a Table, Graph, or Dial

This section describes the differences between dial, graph, and table reports and shows sample reports to help you interpret the information they contain.

Table Reports

Table reports display the total count of all variables since the agent's (or the report's) counters were started or reset. For example, if you have an agent on an XYZ-brand router that has been active for 53 days, the value for "total frames forwarded" displayed in the table is the total number of forwarded frames for 53 days. You can reset the counters at any time; counters automatically wrap (return to zero) after reaching a value of 2^{32} -1, or 4,294,967,295.

Dial and Graph Reports

Dial and graph reports track average variable counter values over the poll interval you selected. For example, if you selected "octets" for the variable and 6 seconds for the poll interval, the count of the total octets transmitted over 6 seconds is divided by 6. That number is displayed on the dial or graph every 6 seconds.

The difference between dial and graph reports is that graph reports display historical data, while a dial displays a "snapshot" of the high, average, and current counter values. A graph report allows you to scroll backward and forward through the report history.

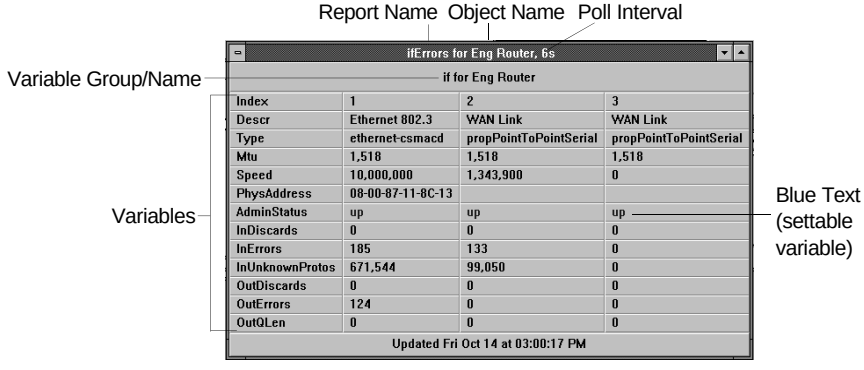
You can change a dial report to a graph report, or vice versa, without restarting the report. See the section titled "Switching from a Dial to a Graph."

Report Samples

This section shows you how to interpret sample table, graph and dial reports.

Sample Table Report

The figure below shows a sample table report:



This report was generated for an object named "Eng Router." The report name (*ifErrors*), the object name (*Eng Router*) and the poll interval (6s) are displayed on the title bar. The variable group name (*if*) and the object name (*Eng Router*) appear above the table.

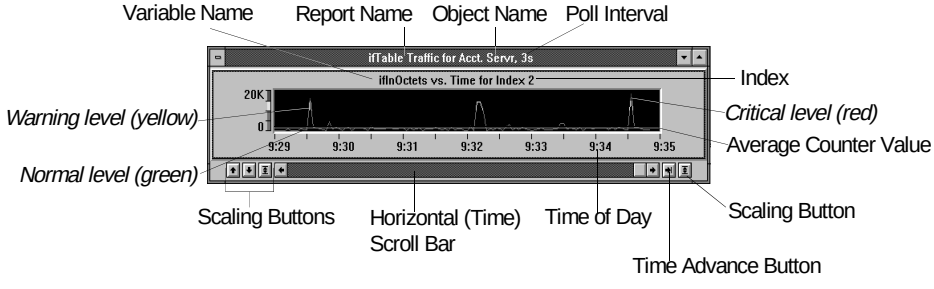
The table contains one row with blue-colored text, indicating the variable (*AdminStatus*) is read-write. Double-clicking on any variable with blue text executes the Set command on that variable. Double-clicking on any variable name displays a description of that variable.

Table Report Text Colors

The color of the counter value text indicates whether or not there is a threshold for that variable and if so, whether the threshold has been exceeded. Black-colored text means there is no threshold; green-colored text means the value is below the Warning threshold; yellow-colored text means the value is above the Warning threshold; and red-colored text means the value is above the Critical threshold.

Sample Graph Report

The figure below shows a sample graph report:



This report was generated for an object named *Acct. Servr*. The report name (*ifTable Traffic*), the object name (*Acct. Servr*) and the poll interval (3s) are displayed on the title bar. The variable name *(inOctets*) and index (*Index 2*) appear at the top of the graph.

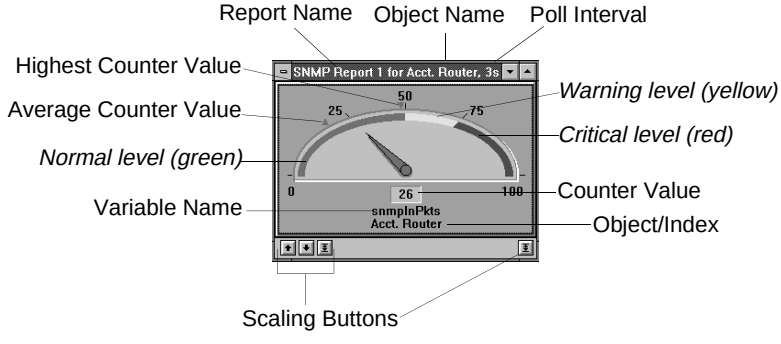
The report also displays the following:

- The color of the line indicates whether the counter value is in a threshold region. A green-colored line means the counter is below the Warning threshold; a yellow-colored line means the counter is above the Warning threshold; and a red-colored line means the counter is above the Critical threshold.

- The average counter value appears as a horizontal line across the graph. The average is calculated for the graph's history since the report was started.
- The time of day is displayed along the horizontal graph axis. More about the time axis on graph reports can be found in the section titled "Expanding or Maximizing Graph Reports" later in this chapter.
- Horizontal and vertical scroll bars appear on any graph report under the following circumstances:
  - A horizontal (time) scroll bar appears after a length of time greater than the elapsed time that can be displayed for the report. You can use this scroll bar to move backward and forward through the entire length of time the report has been open. The report shown on the previous page has a horizontal scroll bar. See Table 5-1, “Default Graph Report Time Intervals” later in this chapter for default elapsed times for graph reports.
  - A vertical scroll bar appears on any multi-graph report when there are more graphs than can fit in one report window

Sample Dial Report

The figure below shows a sample dial report:



This report was generated for an object named *Acct. Router*. The report name (*SNMP Report 1*), the object name (*Acct. Router*) and the poll interval (*3s*) appear on the title bar.

The variable name (*snmpInPkts*) and the object name appear below the counter value. If there was an index associated with the report, the index name would appear in place of the object name below the counter value.

The report also displays the following:

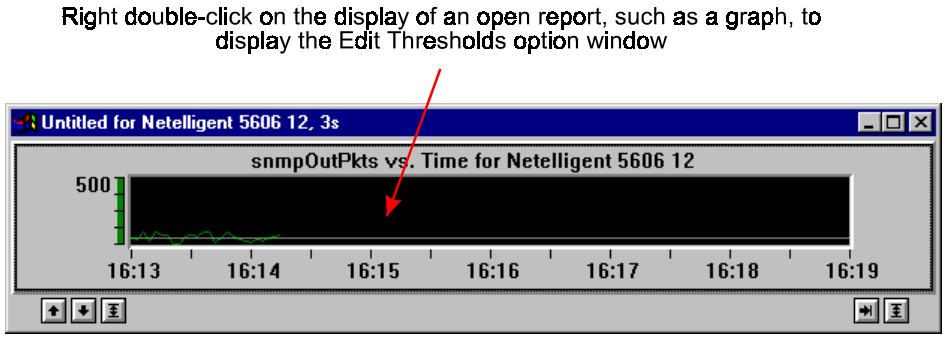
- The current counter value (26 in the figure on the previous page) is displayed below the needle
- The color of the dial needle indicates whether the counter is currently in a threshold region. A green needle means the counter is below the Warning threshold. A yellow needle means the counter is above the Warning threshold; a red needle means the counter is above the Critical threshold.
- Higher and lower arrows on the dial itself indicate the highest and average value for the counter, respectively. The arrows are also colored by the appropriate threshold level.

Editing Report Thresholds

Report *thresholds* are customizable levels that immediately alert you about error conditions on any open report. Report thresholds contain three components: the name of the variable; Warning and Critical threshold values; and the actions to be taken at the occurrence of the Warning and Critical thresholds. This section explains how to edit thresholds and what the threshold options mean.

Editing a Report Threshold by Right Double-Clicking on a Report Display

The simplest way to edit report thresholds is by right double-clicking on the display of any open report:



For multi-index reports, setting thresholds for one index means the same thresholds are used for all other indices in the display. That means you should use some care and not set thresholds too low. If you want to set a threshold for one index that does not affect other indices, restart the same report for the same agent and specify a single index.

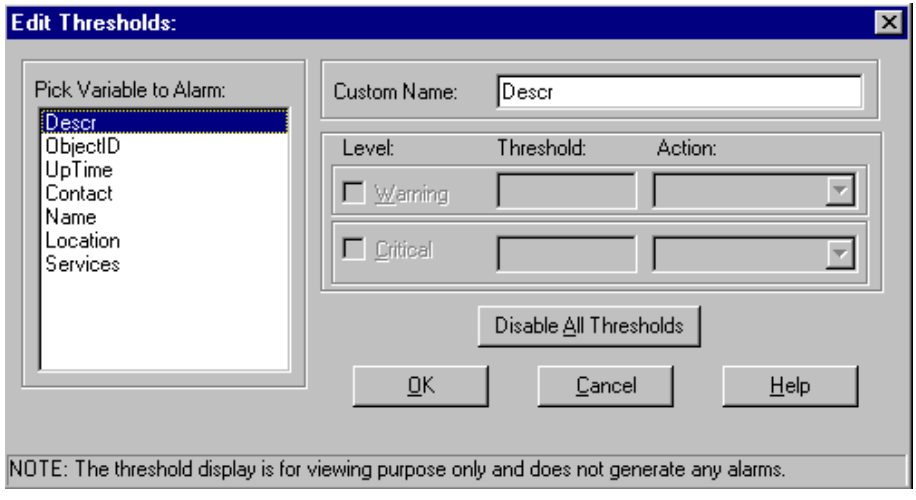
For table reports, right double-clicking on a variable value allows you to set a threshold for that variable. However, not all variables displayed on a table report can have thresholds set for them. That is because table reports can contain MIB variables of any syntax, while only MIB variables of counter or gauge syntax can have thresholds set for them.

Editing a Report Threshold for a Table Report from the Options Menu

Table reports give you a second method to edit thresholds. When a table is the active window, the MIB Browser window in which the table appears contains an Options menu selection. If you select **Edit Thresholds** from this menu, the Edit Thresholds dialog box is displayed.

The Edit Thresholds Dialog Box

A sample Edit Thresholds dialog box is shown below:



- **Pick Variable to Alarm:** A selection box that displays all variables in the report
- **Custom Name:** A text field displaying the name of the variable. You can enter a new variable name in the text field. This new variable name is displayed on this report for this object only. Changing the variable name here does not affect the name of the variable in the agent's MIB.

- **Level:** A combination box that allows you to enable and set thresholds for counter or gauge variables. When you click on a non-counter or non-gauge variable in the Pick Variable to Alarm selection box, the Warning and Critical threshold boxes are grayed-out, indicating you cannot set thresholds. For example, the selected variable in the figure above ("Index") is not counter or gauge syntax, so the Level combination boxes are grayed-out.

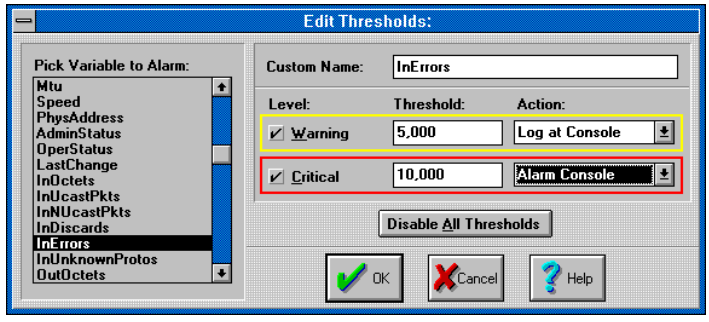
  Checking the Warning or Critical boxes allows you to set Warning or Critical thresholds; unchecking a level means you do not set a threshold. After you check a box, you have the option of entering a value in the Threshold field and of selecting an action from the Action drop-down list.

- **Action**: Options available for most reports are shown below:
  - **Warning**:
    - **Ignore:** Take no action at the occurrence of this threshold.
    - **Show Graph Yellow:** Make a yellow-colored entry
  - **Critical**:
    - **Ignore:** Take no action at the occurrence of this threshold.
    - **Show Graph Yellow:** Make a yellow-colored entry
    - **Show Graph Red :** Make a red-colored entry

  IMPORTANT: Even if you select Ignore for the Action, the report display still reflects the color of the threshold you select. For example, if you select 1,000 for the Warning threshold for a variable, the color of the dial needle, graph line, or the text in the table is yellow when the variable value exceeds 1,000, regardless of the Action you select.

- **Disable All Thresholds button:** Clicking this button clears the Warning and Critical combination boxes. When you return to the report display, any former thresholds for this report is cleared and the report colors do not change.

A sample Edit Thresholds dialog box that sets thresholds for the "*InErrors*" variable is shown in the following figure:



Whenever the value of the *InErrors* variable exceeds 5,000, a yellow-colored message is written to the console log. Whenever the value of *InErrors* exceeds 10,000, a red-colored message is written to the console log.

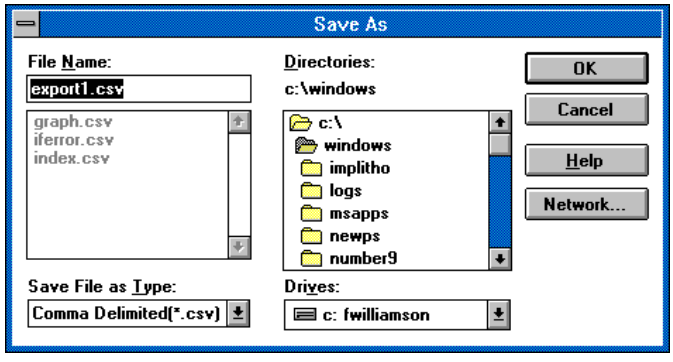
Exporting Report Data

Data from reports can be exported as either comma-delimited or tab-delimited ASCII text. You can use this exported data in a statistics modeling or spreadsheet application to perform detailed analysis.

First, click on an existing report to make it the active window. Then take the following steps:

1. Select **Export Data** from the File menu. The Data Export dialog box similar to the one shown below then appears:

2. Enter a path and a file name in the File Name text field or click the **Select file** button, which displays the Save As dialog box similar to the one shown in the following figure:



3. The Save As dialog box allows you to select the directory and file format for the export. Select a file format from the Save File as Type drop-down list. You can also select either comma-delimited (.CSV) or tab-delimited (.TXT) file format. Clicking on **OK** when you are done returns you to the Data Export dialog box.

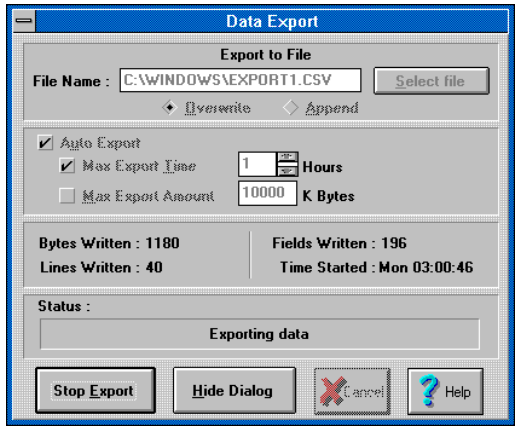
4. If a file with the same name you selected already exists, you can click on the **Overwrite** or **Append** check boxes to replace the existing file or to append the new data at the end of the existing file.

5. The Auto Export check box allows you to select timed, maximum size, or continuous exporting. The options available for auto exporting are shown below:

   - **Max Export Time:** Select a length of time, in hours, to export the report for. After the time interval has elapsed, the export stops.
   - **Max Export Amount:** Select the maximum export file size, in kilobytes (KB). After the export file has reached this size, the export stops.
   - **Continuous (manual stop):** Checking Auto Export but leaving the Max Export Time and Max Export Amount boxes unchecked means the report exports continuously until you stop it by clicking the **Stop Export** button.

6. Once you fill in the dialog box, click on the **Start Export** button to start it. If you did not enable auto exporting, the resulting export is a "snapshot" of the report variables at that time. If you enabled auto exporting for a graph report, the data is exported at the report poll interval multiplied by the condense level. For example, if you selected 6 seconds for the report poll interval and a condense level of 1x, the export file has one row of data every time 6 seconds elapse. (More about condense levels can be found in the section titled "Changing the Condense Level of Graph Reports" later in this chapter.) Report poll intervals are set using the Reports dialog box, as described earlier in this chapter.

7. While the report is exporting, the Data Export dialog box appears similar to the one shown below:



Clicking on the **Hide Dialog** button during an export causes the Export Data dialog box to disappear while the report continues to export. To view the dialog box after it is hidden, select **Export Data** again from the File menu.

Clicking on the **Stop Export** button stops the report from exporting but does not delete the export file. You can click on the **Stop Export** button at any time.

Explanation of Export File

A sample export file is shown below:

```
"ifErrors for Acct. Server, 6s"
"if for Acct. Server"
" ","1"," "," "," "," "," "," "," "," ","2"," "," "," "," "," "," "," "," ","3"," "," "," "," "," "," "," "," ","4"," "," "," "," "," "," "," "," "
"Time","Descr","InOctets","InDiscards"," InErrors","InUnknownProtos","OutOctets","OutDiscards","OutErrors"
,"Descr","InOctets","InDiscards"," InErrors","InUnknownProtos","OutOctets","OutDiscards","OutErrors","Desc
r","InOctets","InDiscards"," InErrors","InUnknownProtos",
"OutOctets","OutDiscards","OutErrors","Descr","InOctets","InDiscards"," InErrors",
"InUnknownProtos","OutOctets","OutDiscards","OutErrors"
"18:22:42","Ether1",376523988,0,29,0,3370689681,0,3480,"Ether2",810903482,0,3,0,2742733260,0,228,
"Ether3",810903482,0,3,0,2742733260,0,228,"Token1",1422446142,0,0,0,787581553,0,476
"18:22:48","Ether1",376524856,0,29,0,3370691222,0,3480,"Ether2",810909392,0,3,0,2742733546,0,228,
"Ether3",810909392,0,3,0,2742733546,0,228,"Token1",1422446142,0,0,0,787581765,0,476
```

This sample export file is explained in the following paragraphs.

First Line

The first line in the export, shown below, corresponds to the title bar of a report display:

```
"ifErrors for Acct. Server, 6s"
```

The name of the report is "ifErrors." The name of the object is "Acct. Server", and the report poll interval is 6 seconds.

Second Line

The second line of the report, shown below, has the variable group name and the name of the object:

"if for Acct. Server"

The variable group name is "if" ("interfaces" in MIB-2), and the name of the object is "Acct. Server."

Indices

If the report covers multiple indices, the indices are listed in the next section of the report, as shown below:

"","1","","","","","","","","","","2","","","","","","","","","","3","","","","","","","","","","4","","","","","","","","","

Each quote-comma-quote (",") represents one report variable. If the report covers only one index, this section is omitted.

Variable Names

The next section in the export file names all the variables in the report. If the report covers more than one index, the variables are listed once for each index. The variable section appears similar to the one shown below:

"Time","Descr","InOctets","InDiscar ds","InErrors","InUnknownProtos","OutOctets","OutDiscard s","OutErrors","Descr","InOctets","InDiscards","InErrors","InUnknownProtos","OutOctets","Out Discards","OutErrors","Descr","InOctets","InDiscards","InErrors","InUnknownProtos", "OutOctets","OutDiscar ds","OutErrors","Descr","InOctets","InDiscards","InErrors", "InUnknownProtos","OutOctets","OutDiscards","OutErrors"

The first field, "Time," is the time of day of the export, and appears only once. The list of report variables, which start with "Descr" and continue through "OutErrors" in the sample above, appear once for each index. Since the report used as an example in this section has four indices, the variables appear four times.

Variable Values

The final section in the export shows variable values, and appears similar to the one shown below:

```
"18:22:42","Ether1",376523988,0,29,0,3370689681,0,3480,"Ether2",810903482,0,3,0,
2742733260,0,228,"Ether3",810903482,0,3,0,2742733260,0,228,"Token1",1422446142,
0,0,0,787581553,0,476
```

The variable values correspond one-for-one to the variable names listed in the previous section of the export. The first field is always the time of day.

Working With Dial and Graph Reports

This section shows you how to make any of the following changes to dial or graph report displays:

Graph reports only:

- Expanding or maximizing graph reports
- Changing the condense level of graph reports

Dial or graph reports:

- Changing the scale of dial or graph reports
- Switching from a dial to a graph
- Using logarithmic scaling
- View Selected/View All on multi-display reports

Expanding or Maximizing Graph Reports

There are three ways to expand the view of a graph report: by selecting a condense level; by stretching it horizontally and/or vertically; and by maximizing it.

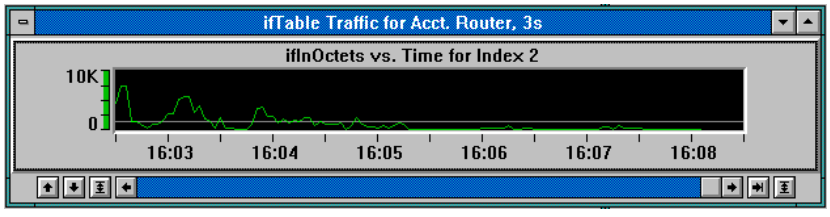
Selecting a condense level for a report changes the time intervals on the horizontal time axis of the report without affecting the size of the display. More about the condense level can be found in the section titled "Changing the Condense Level of Graph Reports."

Stretching a graph report horizontally allows you to view a longer elapsed time on the report without changing its condense level. Vertically expanding a report allows you to view more detail in the graph peaks. Maximizing the report is a convenient way of fully expanding a graph report vertically and horizontally at the same time, so you can view the maximum length of elapsed time and the maximum graph detail.

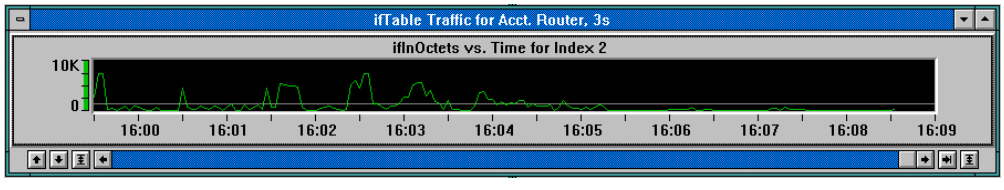
Expanding a Graph Vertically and Horizontally

To expand a report horizontally and/or vertically, click on one edge of a report and drag it. Release the left mouse button and the report expands in the direction(s) in which you dragged it. Or, click on a corner expand it horizontally and vertically at the same time.

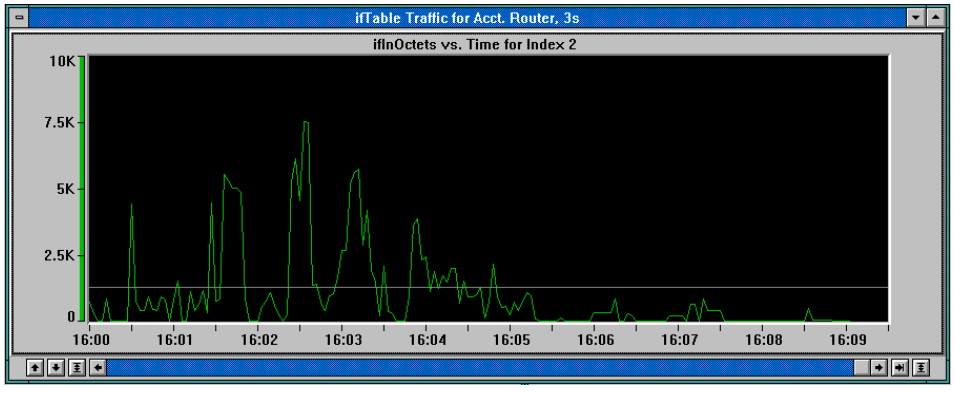
The figure below shows a sample report at its default size:



Expanding the report horizontally displays the total elapsed time for the report as 8.5 minutes, instead of the default 6 minutes as shown in the figure above.

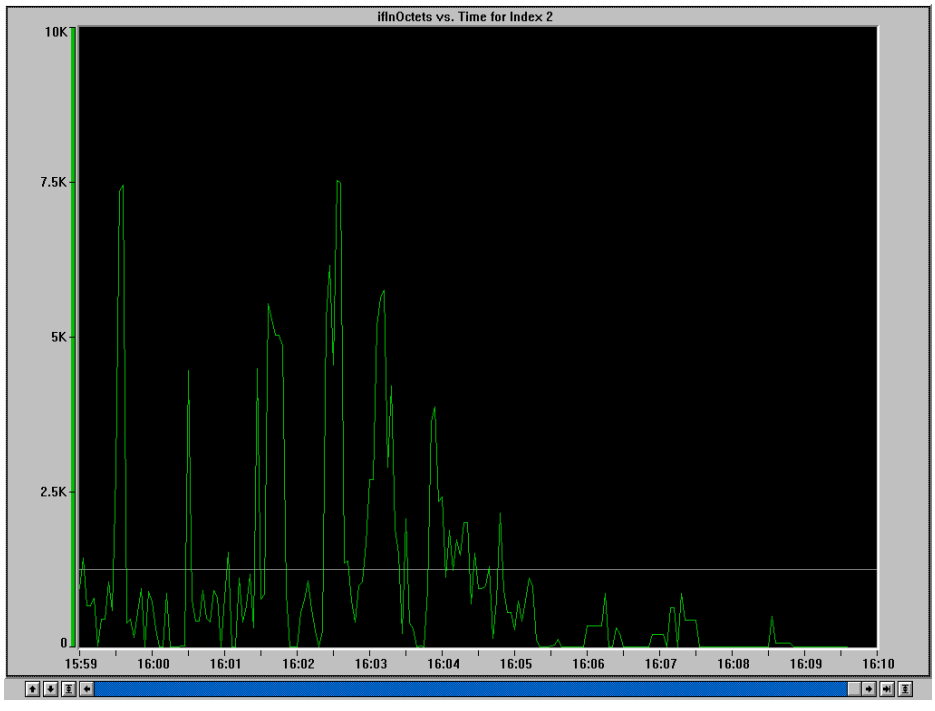


The following figure shows the effect of expanding the same report vertically:


ifTable Traffic for Acct. Router, 3s
ifInOctets vs. Time for Index 2
10K
7.5K
5K
2.5K
0
16:00
16:01
16:02
16:03
16:04
16:05
16:06
16:07
16:08
16:09

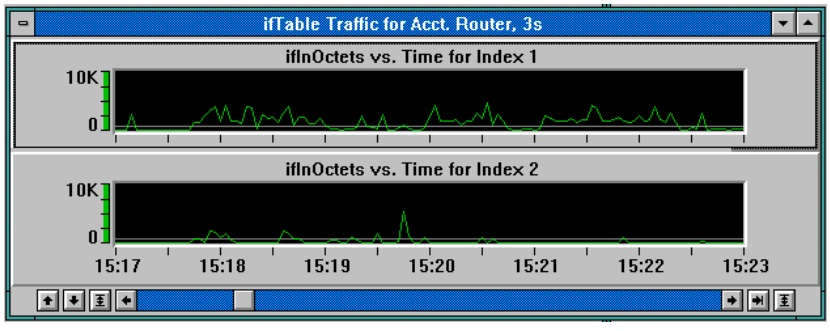
Maximizing a Report

If you want to display the maximum detail possible on a report, maximize it by clicking the maximize button at the top right corner of the report window. A sample graph after maximizing is shown below:

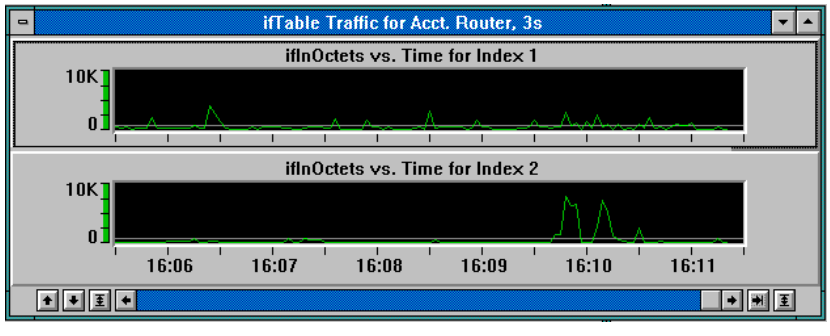


Using the Time Advance Button

In the figure below, the horizontal scroll bar at the bottom of the graph lets you scroll backward and forward through the length of time the report has been open. Suppose you scrolled back to 3:17 p.m. in the report shown below:



Clicking on the time advance button (located next to the right arrow button on the horizontal scroll bar) causes the display to jump to the last time tick on the report, as shown in the figure below:



Changing the Condense Level of Graph Reports

When a graph report is the active window, the Condense View option on the View menu allows you to view a longer total elapsed time on the graph. By default, all graph reports display a total length of time equal to the poll interval multiplied by 20. There are 12 labeled time tick marks on each graph.

Table 5-1 shows the total length of time and the frequency of the labeled tick marks displayed by default on a graph report:

Table 5-1
Default Graph Report Time Intervals

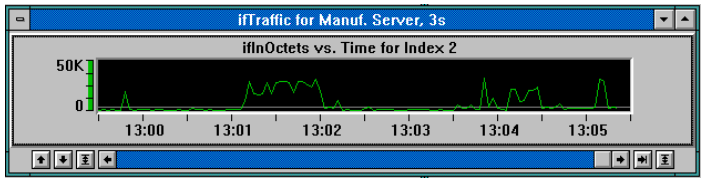
Poll Interval	Total Time Displayed	Frequency of Labeled Time Ticks
3s	6 minutes	every 1 minute
6s	12 minutes	every 1 minute
30s	60 minutes (1 hour)	every 5 minutes
60s	120 minutes (2 hours)	every 10 minutes

Selecting **Condense View** allows you to change these default intervals by a factor of 1 (the default), 6, 12, and 24. Table 5-2 shows how the Condense View option (also called the *condense level*) affects the length of time displayed by default on the graph report:

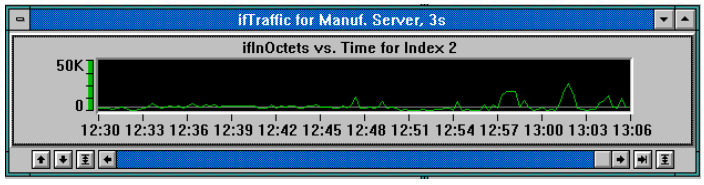
Table 5-2
Effect of Condense Level on Total Report Time

Poll Interval	Condense Level	Total Time Displayed
3s	1x	6 minutes
	6x	36 minutes
	12x	72 minutes (1h, 12m)
	24x	144 minutes (2h, 24m)
6s	1x	12 minutes
	6x	72 minutes (1h, 12m)
	12x	144 minutes (2h, 24m)
	24x	288 minutes (4h, 48m)
30s	1x	60 minutes (1h)
	6x	360 minutes (6h)
	12x	720 minutes (12h)
	24x	1440 minutes (24h)
60s	1x	120 minutes (2h)
	6x	720 minutes (12h)
	12x	1440 minutes (24h)
	24x	2880 minutes (48h)

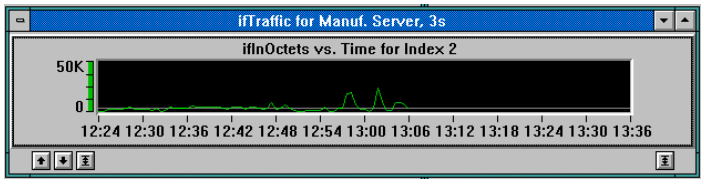
The four following figures illustrate the effect of making selections from the Condense View sub-menu. The first figure shows a report with a poll interval of 3s displayed at the default condense level of **1x**:



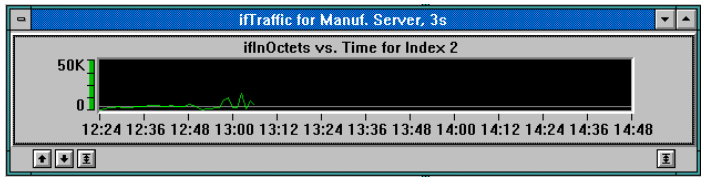
The next figure shows the change to the report after selecting **6x** for the condense level. The total time displayed is 36 minutes.



The figure below shows the change to the report after selecting **12x** for the condense level. The total time displayed is 72 minutes (1 hour, 12 minutes).

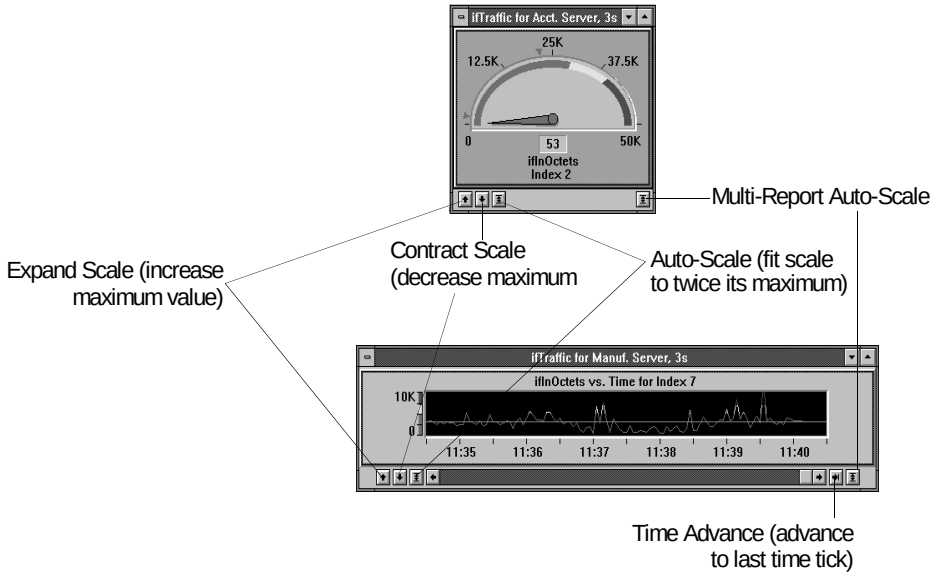


The figure below shows the change to the report after selecting **24x** for the condense level. The total time displayed is 144 minutes (2 hours, 24 minutes).



Changing the Scale of Dial or Graph Reports

Every dial or graph report has buttons that allow you to scale the report display range to fit the range of the report data. The figure below shows a sample dial and graph report with the scaling and time advance buttons labeled:



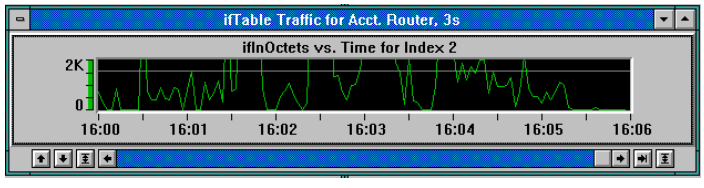
The scaling and time advance buttons contain the functions described below:

- **Expand Scale button:** Doubles the maximum value for the report in units of 20, 50, 100, 200, 500, 1K, etc. each time you click the button
- **Contract Scale button:** Halves the maximum value for the report in units of 2K, 1K, 500, 200, 100, 50, 20 each time you click the button

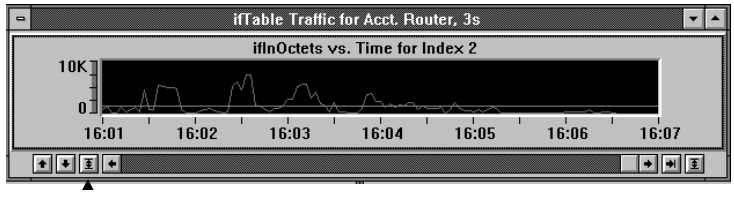
- **Selected Report Auto-Scale button:** Fits the scaling of the report to twice the maximum value, in increments of 50, 100, 200, 500, etc. For example, if the report's maximum value is over 100, clicking the auto-scale button causes the maximum scale of the report to change to 200. For graph reports, the maximum value used for auto-scaling is the maximum for the entire report history.
- **Multi-Report Auto-Scale button:** For reports that display several variables in one report window, clicking this button is equivalent to clicking the auto-scale button for the selected report. For reports that display one variable, this button is equivalent to the auto-scale button. For graph reports, the maximum value used for auto-scaling is the maximum for the entire report history.
- **Advance to Last Time Tick button:** Advances the graph report to the last time tick. This button is useful if you want to review previous report data, then quickly advance to the current time.

Examples of Using the Scaling Buttons

A sample report is shown below:

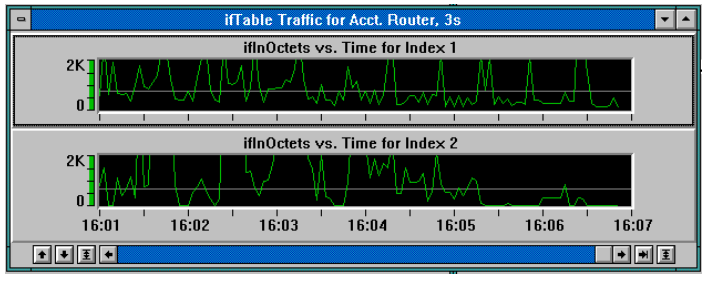


Notice that the data in the graph above does not fit within the report scale; the tops of many peaks are cut off. Clicking on the auto-scale button then increases the maximum value for the report from 2K (as shown on the previous page) to 10K as shown in the following figure:



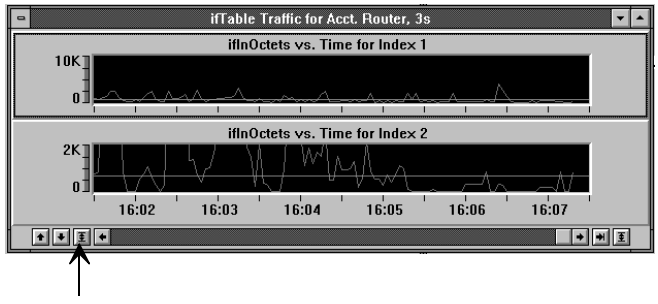
Example of Multi-Variable Report Scaling

Some reports (such as multi-index reports or multi-variable reports) display reports for several indices (or variables) in one report window. For these reports, you can either scale all included reports at once or you can scale them individually. For example, a sample report for two indices is shown below:

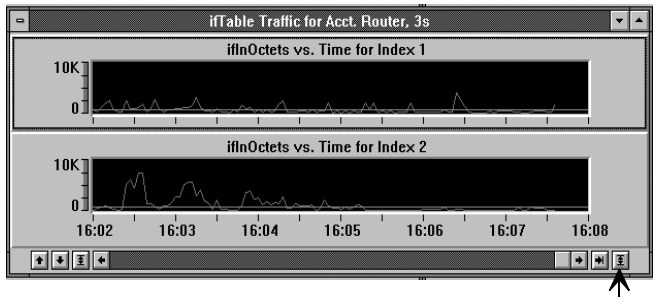


Within the report window, the "active" graph is indicated by a black border (in the figure above, it is the top graph).

Clicking on the selected report auto-scale button re-scales only the active graph, as shown in the following figure:



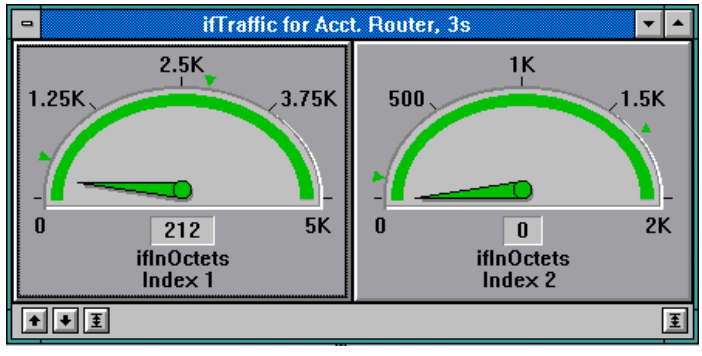
Clicking the multi-report auto-scale button rescales both graphs in the window, as shown below:

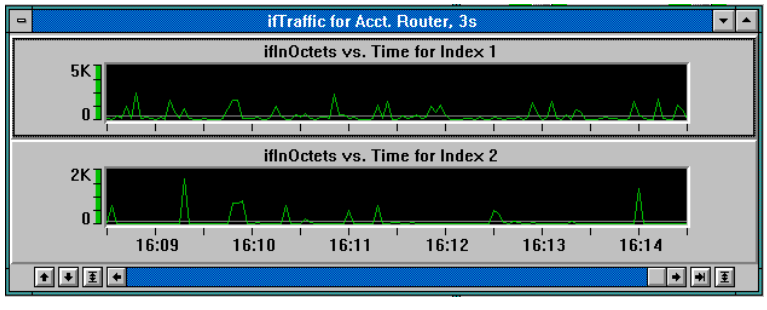


Switching from a Dial to a Graph

When a dial or graph report is the active window, the Dial/Graph option on the View menu allows you to change a report display from a dial to a graph, or vice versa. When you change a report from a dial to a graph, the graph's historical data begins with the time you started the report.

The figures below show the effect of changing a sample report from a dial to a graph:





Using Logarithmic Scaling

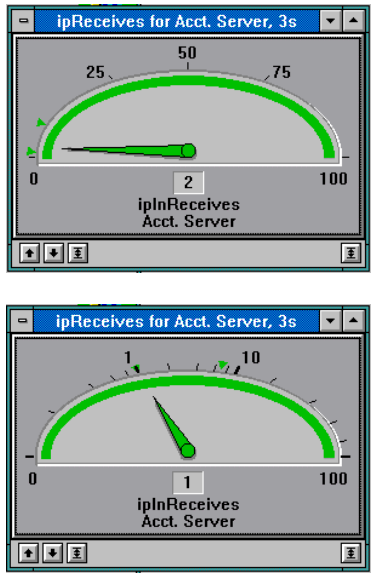
When a dial or graph report is the active window, the Log Scale option on the View menu changes the units of the counter display from linear to logarithmic (Base 10). When you select **Log Scale** from the View menu, a check mark appears beside the option. To change the counter scale back to linear units, uncheck the **Log Scale** option. All reports by default display counter units in linear scale.

When set to the default linear scale, the report's labeled counter tick marks are at 1/4, 1/2, and 3/4 of the maximum displayed. When set to log scale, the labeled tick marks are 1/10 and 1/100 of the maximum displayed. For example, if a report has 1K as its maximum, the labeled counter tick marks in linear scale is 750, 500 and 250. In logarithmic scale, the labeled counter tick marks are 100 and 10. Sample reports are shown on the next page.

Log scale units are appropriate whenever the counter value stays near the low end of the displayed range. For example, if the displayed counter maximum is 100 as shown in the sample reports on the next page, and the counter values stay between 0 and 10, the Log Scale option is more sensitive to small changes in the counter than is the linear scale.

Log scale units are *not* appropriate for reports where there is a wide variation in counter values because then the upper range of the display is less sensitive to changes in counter values.

The two figures shown below show the same report with linear and log scaling:



The displayed maximum for both sample reports is 100; it does not change when you switch from linear to log scale. The labeled tick marks on the top report with linear scale are 25, 50 and 75, which are 1/4, 1/2 and 3/4 of the maximum (100), while the labeled tick marks on the bottom report (1 and 10) are 1/10 and 1/100 of the maximum.

Since the counter values remain near the low end of the report's range, the log scale viewing option is more sensitive to the movement of the dial pointer. If the counter goes much above 10, it is a good idea either to increase the maximum on the report or to switch back to linear scaling.

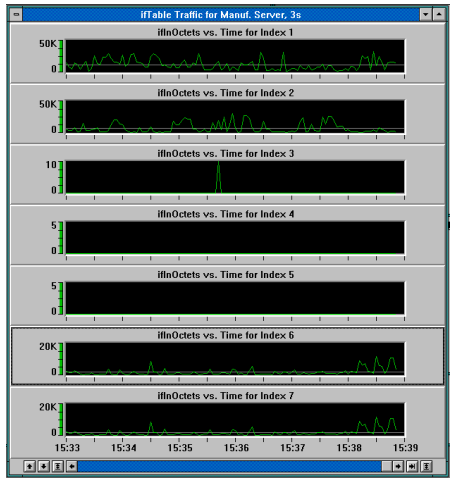
View Selected/View All on Multi-Display Reports

These options are available only for multi-display dial or graph reports. *Multi-display* reports are created under either of the following circumstances:

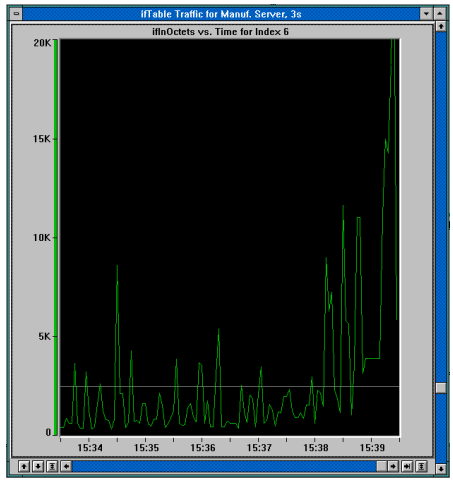
- More than one variable is selected or displayed. For example, you can create a custom report by selecting more than one variable in the Browser; or you can start an existing report that includes more than one variable, such as the "icmp" report for MIB-2.
- More than one index is involved. For example, if you create an "IfInOctets" report for an object with five indices (for each of five adapters in a server, for example), the resulting report displays five individual dials or graphs.

The two sample reports on the next page show the difference between viewing all displays on a multi-display report, and viewing a selected display.

Viewing all displays:



Viewing a selected display:



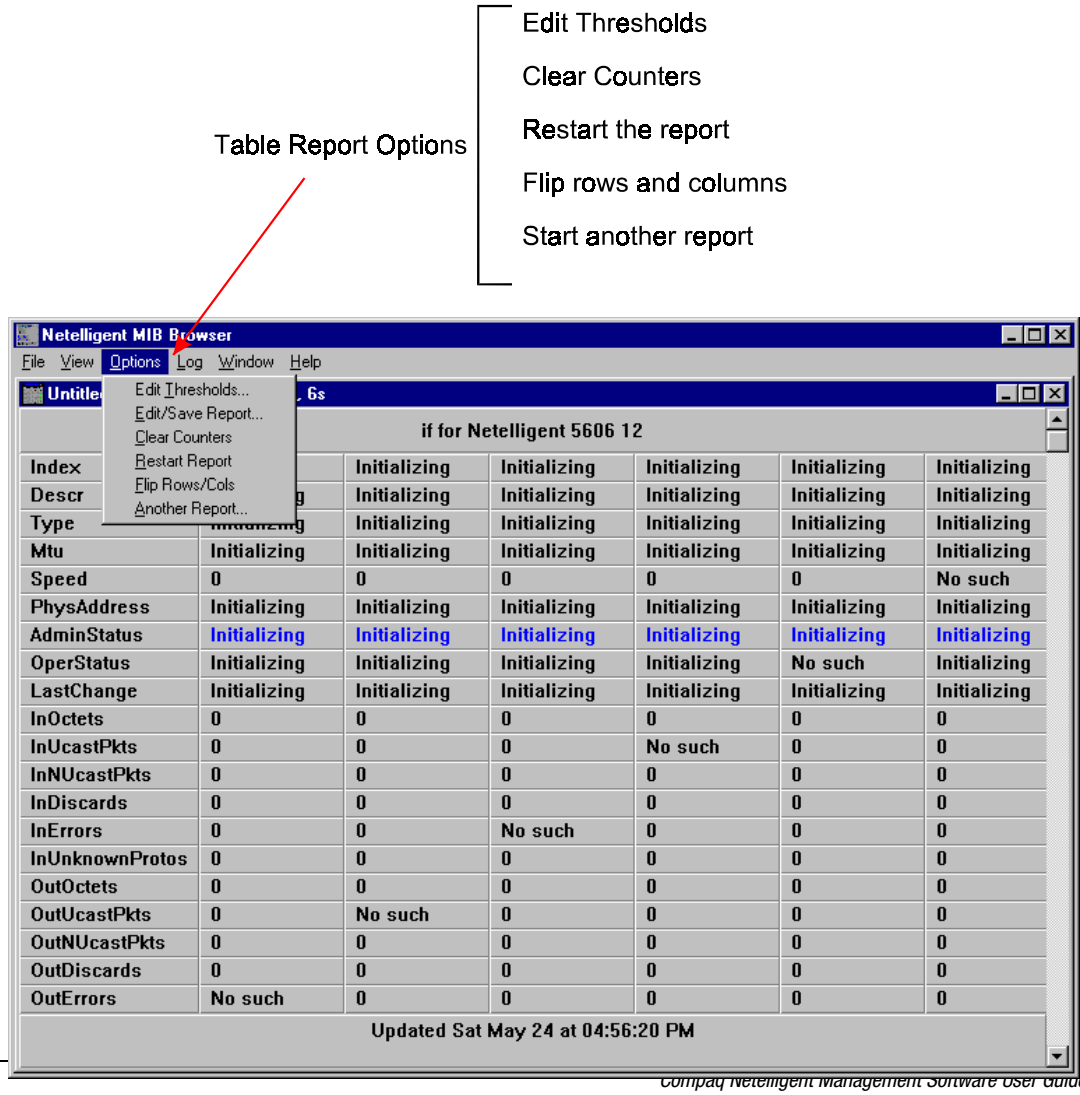
The top report displays seven graphs in the window, for each of seven indices.

There are two ways to view a selected display:

- Left double-clicking on the display you wish to view
- Left clicking once on the display then choosing **View Selected** from the View menu (the selected display has a black border around it after you click on it)

Working With Table Reports

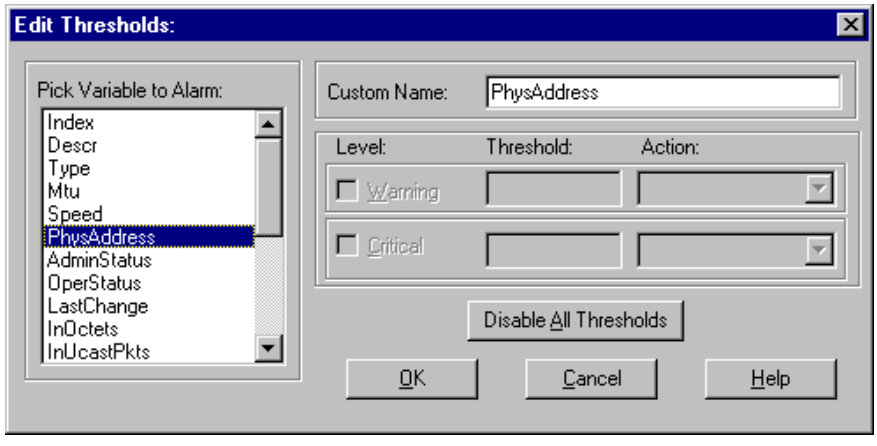
This section shows you how to perform actions on table reports as shown in the illustration below:



Index	Initializing	Initializing	Initializing	Initializing	Initializing	Initializing
Descr	Initializing	Initializing	Initializing	Initializing	Initializing	Initializing
Type	Initializing	Initializing	Initializing	Initializing	Initializing	Initializing
Mtu	Initializing	Initializing	Initializing	Initializing	Initializing	Initializing
Speed	0	0	0	0	0	No such
PhysAddress	Initializing	Initializing	Initializing	Initializing	Initializing	Initializing
AdminStatus	Initializing	Initializing	Initializing	Initializing	Initializing	Initializing
OperStatus	Initializing	Initializing	Initializing	Initializing	No such	Initializing
LastChange	Initializing	Initializing	Initializing	Initializing	Initializing	Initializing
InOctets	0	0	0	0	0	0
InUcastPkts	0	0	0	No such	0	0
InNUcastPkts	0	0	0	0	0	0
InDiscards	0	0	0	0	0	0
InErrors	0	0	No such	0	0	0
InUnknownProtos	0	0	0	0	0	0
OutOctets	0	0	0	0	0	0
OutUcastPkts	0	No such	0	0	0	0
OutNUcastPkts	0	0	0	0	0	0
OutDiscards	0	0	0	0	0	0
OutErrors	No such	0	0	0	0	0

Edit Thresholds

Selecting **Edit/Thresholds** from the Options menu when a table report is the active window displays the Thresholds dialog box.Need to change the screen capture.

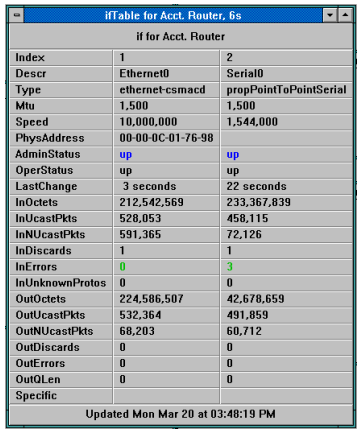


Clearing Report Counters

Selecting **Clear Counters** from the Options menu when a table report is the active window sets the values of all table report counters to zero. Since table reports contain cumulative statistics, this option is useful if the report counters are at a very high value, or if you want to get an idea of how quickly the counters are incrementing. Selecting this option does not affect any statistics counters at the agent; it resets the counters on your report display only.

The two figures below illustrate the effect of selecting **Clear Counters**.

Before selecting **Clear Counters**:



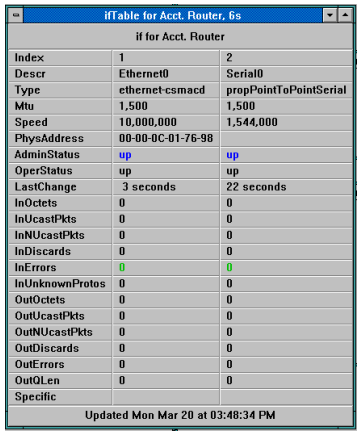
ifTable for Acct. Router, 6s

if for Acct. Router

Index	1	2
Descr	Ethernet0	Serial0
Type	ethernet-csmacd	propPointToPointSerial
Mtu	1,500	1,500
Speed	10,000,000	1,544,000
PhysAddress	00-00-0C-01-76-98	
AdminStatus	up	up
OperStatus	up	up
LastChange	3 seconds	22 seconds
InOctets	212,542,569	233,367,839
InUcastPkts	528,053	458,115
InNUcastPkts	591,365	72,126
InDiscards	1	1
InErrors	0	3
InUnknownProtos	0	0
OutOctets	224,586,507	42,678,659
OutUcastPkts	532,364	491,859
OutNUcastPkts	68,203	60,712
OutDiscards	0	0
OutErrors	0	0
OutQLen	0	0
Specific		

Updated Mon Mar 20 at 03:48:19 PM

After selecting **Clear Counters**:



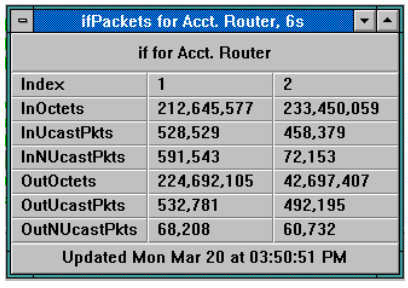
Restarting the Report

Selecting **Restart Report** from the Options menu when a table report is the active window reinitializes a table report, as if you were starting the report anew. You might use this option for reports containing information that might change (such as reports that show MAC addresses or indices, both of which are subject to change with time).

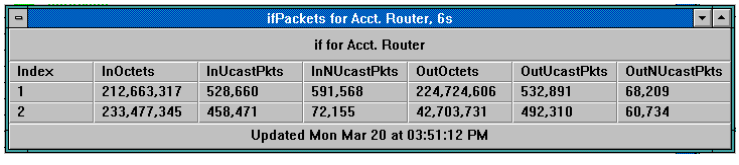
Flipping Rows and Columns

Selecting **Flip Rows/Cols** from the Options menu when a table report is the active window causes the fields that define columns to define rows, and vice versa. (Selecting this option again restores the columns and rows to their original orientations.) The two figures below illustrate the effect of this option.

Before selecting **Flip Rows/Cols**:



After selecting **Flip Rows/Cols**:


ifPackets for Acct. Router, 6s
if for Acct. Router
Index InOctets InUcastPkts InNUcastPkts OutOctets OutUcastPkts OutNUcastPkts
1 212,663,317 528,660 591,568 224,724,606 532,891 68,209
2 233,477,345 458,471 72,155 42,703,731 492,310 60,734
Updated Mon Mar 20 at 03:51:12 PM

Starting Another Report

Selecting **Another Report** from the Options menu when a table report is the active window allows you to start another report. After selecting this option, the Reports dialog box appears.

All existing reports for the merged MIB are displayed in the Select Report selection box.

Click on the report you wish to start and click the **Start Report** button. If you want more information about this dialog box, click on the **Help** button to access the online help.

Table Report Shortcuts

The right and left mouse buttons can be used with report displays to obtain additional information about table report variables; to quickly execute a Set command on a read-write MIB variable; or to edit report thresholds. Two examples are shown in this section.

Shortcut 1: Getting Additional Information about a Table Variable

To find additional information about a variable in a table report, left double-click on the variable name. A sample table report is shown below:

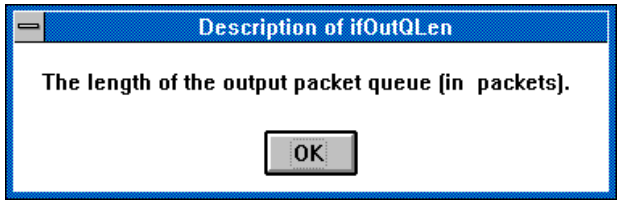
ifTable for Acct. Router, 6s

if for Acct. Router

Index	1	2
Descr	Ethernet0	Serial0
Type	ethernet-csmacd	propPointToPointSerial
Mtu	1,500	1,500
Speed	10,000,000	1,544,000
PhysAddress	00-00-0C-01-76-98	
AdminStatus	up	up
OperStatus	up	up
LastChange	3 seconds	22 seconds
InOctets	1,245,310	1,770,543
InUcastPkts	6,901	4,020
InNUcastPkts	1,966	257
InDiscards	0	0
InErrors	0	0
InUnknownProtos	0	0
OutOctets	2,161,801	282,067
OutUcastPkts	6,828	4,618
OutNUcastPkts	57	199
OutDiscards	0	0
OutErrors	0	0
OutQLen	0	0
Specific		

Updated Mon Mar 20 at 04:16:31 PM

Left double-clicking on the *OutQLen* variable in the table shown above reveals the description box shown below:

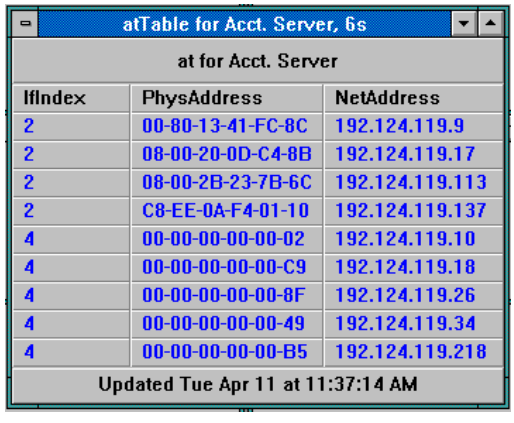


Shortcut 2: Setting a Variable

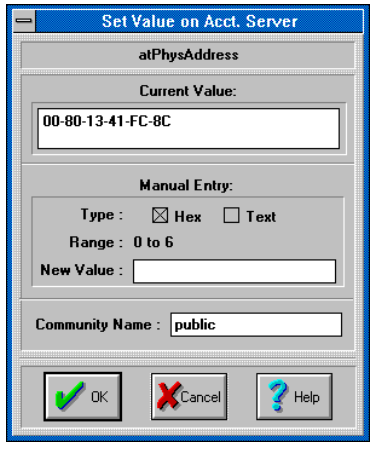
IMPORTANT : Using the Set command changes values of variables at the agent. Before using the command, make sure the value you plan to change does not adversely affect the operation of the agent.

Left double-clicking on a settable (read-write) variable value in a table report allows you to execute a Set command on that variable. Settable variables are displayed in blue text.

For example, the *atTable* report shown below has several settable variables:



Left double-clicking on **00-80-13-41-FC-8C** displays the Set Value dialog box shown below:



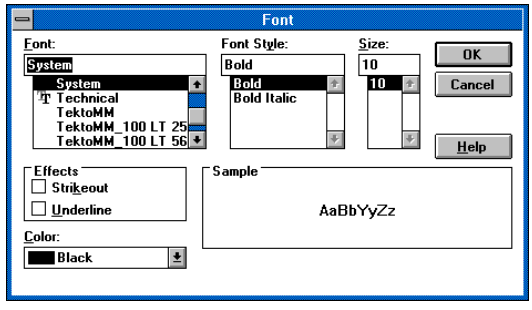
The name of the object (*Acct. Server* in the figure above) appears on the title bar. The full variable name (*atPhysAddress* in the figure above) appears below the title bar. The agent community name you are using to manage the agent (public in the figure above) appears in the Community Name text field.

Since *atPhysAddress* is an octet string, the Set Value dialog box also contains two check boxes, Hex and Text. Click on the box corresponding to the units you wish to set the octet string to and type in a value in the New Value text field and click **OK**.

If the Set command is successful, you the variable value changes in the table report. If the Set command is unsuccessful, the variable value does not change. The most likely reason a Set command fails is that the agent community you are using does not have sufficient rights to the agent.

Selecting a Font

When you select **Set Font** from the View menu when a report display is the active window, a dialog box appears similar to the one shown in the figure below:



The dialog box displays all currently-installed True Type fonts, plus printer fonts for your default Windows printer. Make a selection from this dialog box and click **OK**. Another dialog box then appears which gives you the option of using the same font on all future reports.

Printing a Report

A report display can be printed on any available Windows printer when you select **Print Report** when a report display is the active window.

Closing a Report

Closing a report window stops the collection of statistics. To close a report that is currently open, click on the control menu (located in the upper left-hand corner of the report window). This displays the Control menu for this window. Select **Close** from this menu, as shown below: